Szenarien für den Aufbau eines ViPNet VPN Netzwerks

Anhang zum ViPNet VPN Benutzerhandbuch

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

1991–2015 Infotecs GmbH, Berlin

Version: 00121-04 90 01 DEU

Dieses Dokument ist Teil des Softwarepaketes und unterliegt daher denselben Lizenzbestimmungen wie das Softwareprodukt.

Dieses Dokument oder Teile davon dürfen nicht ohne die vorherige schriftliche Zustimmung der Infotecs GmbH verändert, kopiert, weitergegeben etc. werden.

ViPNet ist ein registriertes Warenzeichen des Softwareherstellers Infotecs GmbH.

Marken

Alle genannten Markennamen sind Eigentum der jeweiligen Hersteller.

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt

Einführung **5**
Über dieses Dokument 6
Zielgruppe 6
Verwendete Konventionen 6
Kontakt 8
FAQ und andere Hilfsinformation 8
Kontakt 8
Allgemeine Hinweise 9
Grundlegende Möglichkeiten beim Aufbau von ViPNet VPN-Netzwerken 11
Bevor Sie mit der Arbeit beginnen 12

Kapitel 1. Verbindungen zwischen Remotebenutzer und Niederlassung **14**
Kurze Übersicht 15
Netzwerkparameter in ViPNet Network Manager einstellen 16
ViPNet Netzwerk einrichten 16
ViPNet Netzwerkparameter konfigurieren 17
Einstellungen auf der Firewall überprüfen 19
Einstellungen auf dem Coordinator überprüfen 20
Einstellungen auf den Clients in der Niederlassung überprüfen 21
Einstellungen auf den Remote-Clients überprüfen 23

Kapitel 2. Verbindungen zwischen zwei Remotebenutzern **25**
Kurze Übersicht 26
Netzwerkparameter in ViPNet Network Manager einstellen 27
Einstellungen auf der Firewall und auf dem Coordinator überprüfen 28
Einstellungen auf den Remote-Clients überprüfen 29

Kapitel 3. Verbindungen zwischen zwei Niederlassungen **31**
Kurze Übersicht 32
Netzwerkparameter in ViPNet Network Manager einstellen 33
Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen 35
Einstellungen der Clients beider Niederlassungen überprüfen 37

Kapitel 4. Verbindungen zwischen zwei Niederlassungen mit Hilfe der Tunnelung **38**
Kurze Übersicht 39
Netzwerkparameter in ViPNet Network Manager einstellen 40

Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen 43
Routing-Einstellungen der getunnelten Knoten überprüfen 46
Einstellungen auf Remote-Clients überprüfen 48

Kapitel 5. Verbindungen zwischen der Niederlassung und dem Benutzer eines mobilen Geräts 50
Kurze Übersicht 51
Netzwerkparameter in ViPNet Network Manager einstellen 53
Konfiguration des Coordinators unter Windows 56
Einstellungen auf externen Firewall überprüfen 58
Konfiguration mobiler Geräte 59
Konfiguration mobiles Geräts von Apple 59
Konfiguration mobiles Geräts von Android 59
Einstellungen auf dem Coordinator unter Windows überprüfen 61

Kapitel 6. Verbindungen zwischen zwei Niederlassungen unter Verwendung von ViPNet und IPsec-Technologie 63
Kurze Übersicht 64
Netzwerkparameter in ViPNet Network Manager einstellen 65
Überprüfen der Einstellungen auf dem Remotegateway 69

Einführung

Über dieses Dokument 6

Kontakt 8

Allgemeine Hinweise 9

Grundlegende Möglichkeiten beim Aufbau von ViPNet VPN-Netzwerken 11

Bevor Sie mit der Arbeit beginnen 12

Über dieses Dokument

Dieses Dokument stellt den Anhang zum „ViPNet VPN. Benutzerhandbuch" dar und beinhaltet die Beschreibung von sechs typischen Möglichkeiten für den Aufbau geschützter ViPNet VPN-Netzwerke. Für jedes Schema sind Schritt-für-Schritt-Anleitungen aufgeführt, mit deren Hilfe die entsprechende Netzwerkstruktur im Programm ViPNet Network Manager zunächst angelegt und konfiguriert werden kann, und anschließend die Einstellungen direkt auf den Netzwerkknoten überprüft werden können.

Zielgruppe

Dieses Handbuch wendet sich an Netzwerkadministratoren, die für den Aufbau und die Konfiguration des VPN-Netzwerks ViPNet VPN verantwortlich sind.

Beim Leser dieses Handbuchs werden keine tiefgehenden Kenntnisse der Netzwerktechnologie vorausgesetzt. Ein gewisses Grundwissen über Computernetzwerke, IP-Protokolle, Firewalls, Tunnelung und Kryptographie kann jedoch hilfreich sein.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.

Notation	Beschreibung
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

Allgemeine Hinweise

Bei der Arbeit mit diesem Handbuch ist es empfehlenswert, folgende Hinweise zu beachten:

1 Wählen Sie ein Szenario, das der benötigten logischen Struktur des privaten Netzwerks entspricht (s. Grundlegende Möglichkeiten beim Aufbau von ViPNet VPN-Netzwerken auf S. 11).

Es sollte beachtet werden, dass, wenn das private Netzwerk zwei Niederlassungen einer Firma verbinden soll, es empfehlenswert scheint, ein einheitliches ViPNet Firmennetzwerk einzurichten und dort alle Rechner der beiden Niederlassungen zu integrieren. Wenn geschützte Verbindungen zwischen zwei unterschiedlichen Organisationen hergestellt werden sollen, ist es empfehlenswert, in jeder Firma ein eigenes ViPNet Netzwerk einzurichten und anschließend Partnernetzwerk-Verbindungen aufzubauen (s. „ViPNet VPN Benutzerhandbuch", Kapitel 6, Abschnitt „Aufbau von Partnernetzwerk-Verbindungen").

Achtung! In diesem Handbuch wird die Interaktion der Computer innerhalb eines einzigen ViPNet Firmennetzwerks beschrieben, das die Haupt- und die Zweigniederlassung miteinander verbindet.

2 Installieren Sie auf der Arbeitsstation des ViPNet Administrators die Software ViPNet Network Manager und ViPNet Client oder ViPNet Coordinator (s. „ViPNet VPN Benutzerhandbuch", Kapitel 2, Abschnitt „Einrichtung des Manager-Arbeitsplatzes").

3 Legen Sie im Programm ViPNet Network Manager die logische Struktur Ihres Netzwerks fest und erstellen Schlüsseldistributionen für die Netzwerkknoten, indem Sie den Anleitungen in diesem Handbuch folgen.

4 Installieren Sie auf den Computern, die als Coordinatoren eingesetzt werden sollen, die Software ViPNet Coordinator (s. „ViPNet VPN Benutzerhandbuch", Kapitel 2, Abschnitt „Installation von ViPNet Coordinator auf ViPNet Netzwerkserver") und die Schlüsseldistributionen, die Sie zuvor in ViPNet Network Manager erstellt haben.

5 Installieren Sie auf den Arbeitsstationen der ViPNet Benutzer (Clients) einschließlich aller Remote-Arbeitsstationen die Software ViPNet Client (s. „ViPNet VPN Benutzerhandbuch", Kapitel 2, Abschnitt „Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk") und die Schlüsseldistributionen, die Sie zuvor in ViPNet Network Manager erstellt haben.

6 Überprüfen Sie die Verbindungen zwischen Coordinatoren und entfernten Benutzern, zwischen unterschiedlichen entfernten Benutzern und zwischen Coordinatoren der verschiedenen Niederlassungen.

7 Wenn keine Verbindungen aufgebaut werden konnten, dann folgen Sie den Anweisungen zur Überprüfung der Einstellungen in den Programmen ViPNet Coordinator und ViPNet Client, die auf Coordinatoren und Clients installiert sind.

Hinweis. Wenn irgendwelche Einstellungen von Coordinatoren oder Clients geändert werden sollen, verwenden Sie dazu das Programm ViPNet Network Manager:

- Wählen Sie in der Navigationsleiste den Netzwerkknoten aus, dessen Einstellungen geändert werden sollen.
- Führen Sie in den Registerkarten des Panel-Ansichts die erforderlichen Einstellungen durch.
- Erstellen Sie Schlüsseldistributionen, kopieren Sie diese auf einen externen Datenträger und installieren Sie diese manuell auf den ViPNet Netzwerkknoten.

8 Überprüfen Sie erneut die Verbindungen zwischen den Netzwerkknoten.

Wenn immer noch keine Verbindungen aufgebaut werden können, kann die Ursache in der Inkompatibilität der Softwareversionen oder in den Einstellungen der Firewall liegen. Wenden Sie sich an den technischen Support der Firma „Infotecs".

Grundlegende Möglichkeiten beim Aufbau von ViPNet VPN-Netzwerken

Nachfolgend sind sechs typische Installationsschemas für das ViPNet VPN-Netzwerk aufgeführt:

1 Verbindungen zwischen Remotebenutzer und Niederlassung (auf S. 14)

Verwenden Sie dieses Szenario, um ein ViPNet Netzwerk zu installieren, das Verbindungen zwischen entfernten Benutzern und der Niederlassung ermöglicht. Der Remotebenutzer kann auf einem Notebook arbeiten und sich über das Internet (zu Hause, im Cafe usw.) mit dem ViPNet Netzwerk verbinden. Der Remotebenutzer kann auch auf einem Desktop-PC arbeiten (zu Hause oder an einem anderen Ort), von dem keine direkte Verbindung zum Coordinator aufgebaut werden kann.

2 Verbindungen zwischen zwei Remotebenutzern (auf S. 25)

Verwenden Sie dieses Schema, um ein ViPNet Netzwerk mit zwei entfernten Benutzern zu installieren, die miteinander kommunizieren sollen.

3 Verbindungen zwischen zwei Niederlassungen (auf S. 31)

Verwenden Sie dieses Schema, um ein ViPNet Netzwerk zu installieren, das geschützte Verbindungen zwischen Computern mit installierter ViPNet Software, die sich in unterschiedlichen Niederlassungen befinden, ermöglichen soll.

4 Verbindungen zwischen zwei Niederlassungen mit Hilfe der Tunnelung (auf S. 38)

Verwenden Sie dieses Schema, um ein ViPNet Netzwerk aufzubauen, das geschützte Verbindungen zwischen Computern, die sich in unterschiedlichen Niederlassungen befinden, auch dann ermöglichen soll, wenn auf diesen Computern keine ViPNet Software installiert ist. Es kann sich dabei um Rechner mit unterschiedlichen Betriebssystemen, Netzwerkdrucker, VoIP-Geräte, NAS-Geräte, IP-Kameras usw. handeln.

5 Verbindungen zwischen der Niederlassung und dem Benutzer eines mobilen Geräts (auf S. 50)

Verwenden Sie dieses Schema, um ein ViPNet Netzwerk zu erstellen und Verbindungen zwischen den Benutzern mobiler Geräte von Apple oder Android und der Niederlassung einzurichten.

6 Verbindungen zwischen zwei Niederlassungen unter Verwendung von ViPNet und IPsec-Technologie (auf S. 63)

Verwenden Sie dieses Schema, um ein ViPNet Netzwerk zu erstellen und eine Partnernetzwerk-Verbindung zu einem anderen Netzwerk einzurichten, in dem keine ViPNet Technologie verwendet wird.

Bevor Sie mit der Arbeit beginnen

Legen Sie rechtzeitig fest, auf welchem Computer die Software ViPNet Coordinator (Server im ViPNet Netzwerk) und auf welchem Computer ViPNet Client (Arbeitsstation des ViPNet Netzwerkbenutzers) installiert werden sollen. Der Coordinator muss jederzeit für alle seine Clients erreichbar sein. Das heißt, er sollte immer aktiv und an das Netzwerk angeschlossen sein. Auf der Firewall, die der Coordinator für den Zugang zum Internet verwendet, sollte die Konfiguration von Regeln zur Umleitung des Traffics möglich sein.

Installieren Sie mit Hilfe der Installationsdatei von ViPNet VPN die Software ViPNet Network Manager und ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz (s. „ViPNet VPN Benutzerhandbuch", Kapitel 2, Abschnitt „Erstellen des Manager-Arbeitsplatzes"). Mit Hilfe des Programms ViPNet Network Manager wird die Einrichtung, die Konfiguration und die Administration des privaten ViPNet Netzwerks, welches Computer in der Hauptniederlassung und in den Filialen sowie entfernte Computer umfassen kann, durchgeführt.

Damit Verbindungen zwischen den Computern der Niederlassung und den Computern in den Filialen bzw. entfernten Computern möglich sind, sollte im ViPNet Netzwerk zumindest ein Coordinator installiert werden, der jederzeit von außen über eine externe (öffentliche) IP-Adresse oder über einen DNS-Namen erreicht werden kann. In den ersten beiden und letzten beiden in diesem Dokument beschriebenen Szenarien übernimmt diese Rolle der einzige Coordinator im Netzwerk. In den dritten und vierten Szenarien ist dies der Coordinator in der Niederlassung.

Falls der Coordinator über keine statische öffentliche IP-Adresse verfügt, verwenden Sie einen dynamischen DNS-Dienst, der externe dynamische IP-Adressen der Firewall in einen vordefinierten DNS-Namen umwandelt (zum Beispiel www.dynDNS.com).

Achtung! Bevor Sie mit der Konfiguration der Parameter von ViPNet Netzwerkknoten beginnen, führen Sie die nachfolgend beschriebenen Schritte durch.

- Vergewissern Sie sich, dass der Netzwerkadapter des Coordinators, der mit der Firewall verbunden ist, über eine statische lokale IP-Adresse verfügt.
- Stellen Sie sicher, dass Sie die externe statische IP-Adresse oder den DNS-Namen des Coordinators in der Niederlassung kennen.
- Stellen Sie sicher, dass auf den Firewalls, hinter denen sich die Coordinatoren befinden, folgende Regeln konfiguriert sind: eingehenden Traffic auf dem in den Coordinatoreinstellungen definierten UDP-Port (standardmäßig Port 55777) erlauben und an die lokale IP-Adresse des Coordinators weiterleiten.

  Führen Sie die folgenden Schritte durch, um zu erfahren, welcher Port auf dem Coordinator für die Kapselung der UDP-Pakete festgelegt ist:

  - Wählen Sie im Hauptfenster des Programms **ViPNet Coordinator [Monitor]** im Menü **Service** den Befehl **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.

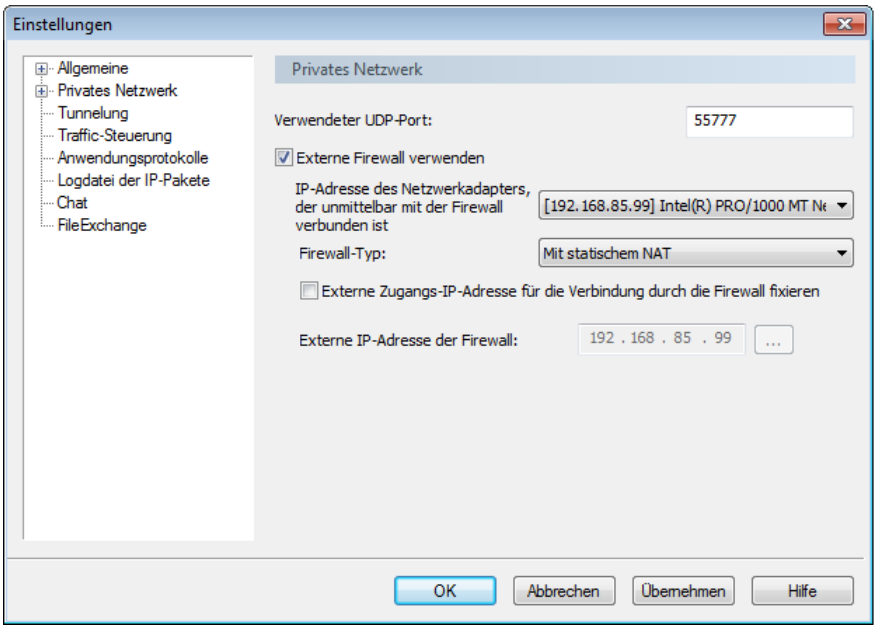

Abbildung 1. Port für die Kapselung der UDP-Pakete überprüfen

- Die Portnummer wird im Bereich **Privates Netzwerk** im Feld **Verwendeter UDP-Port** festgelegt.

1

Verbindungen zwischen Remotebenutzer und Niederlassung

Kurze Übersicht 15

Netzwerkparameter in ViPNet Network Manager einstellen 16

Einstellungen auf der Firewall überprüfen 19

Einstellungen auf dem Coordinator überprüfen 20

Einstellungen auf den Clients in der Niederlassung überprüfen 21

Einstellungen auf den Remote-Clients überprüfen 23

Kurze Übersicht

Dieses Kapitel beschreibt das Schema eines ViPNet VPN-Netzwerks, in dem ein Remotebenutzer Verbindungen zur Firmenniederlassung aufbaut. Der Remotebenutzer kann auf einem Notebook arbeiten, indem er sich aus der Niederlassung oder über das Internet (zu Hause, im Cafe usw.) mit dem ViPNet Netzwerk verbindet. Ebenso kann der Remotebenutzer einen stationären Computer zu Hause oder an einem andern Ort verwenden, von welchem keine direkten Verbindungen zum Coordinator möglich sind.

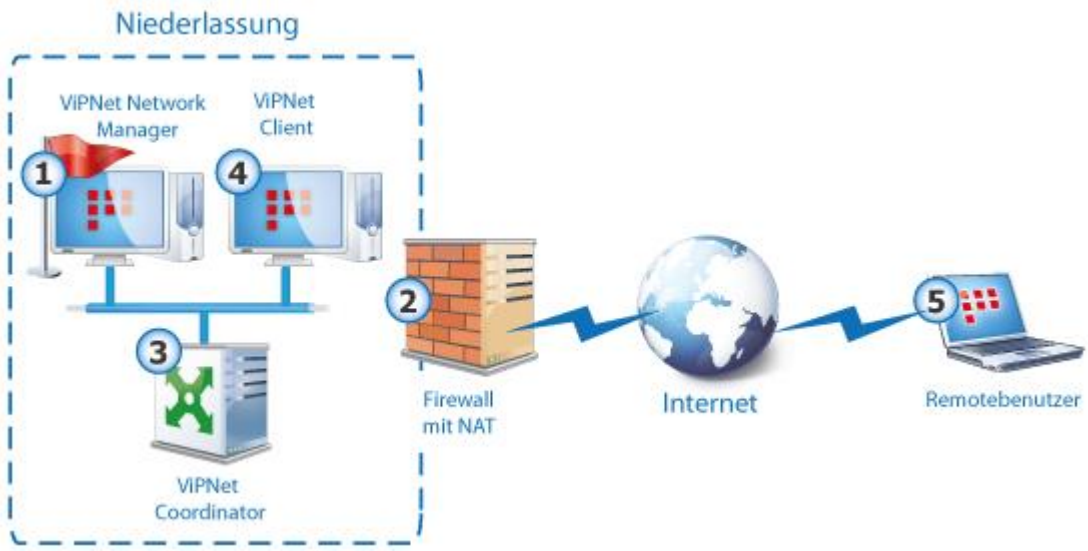

Abbildung 2. Verbindung zwischen einem Remotebenutzer und der Firmenniederlassung

Nehmen wir an, dass sich in der Niederlassung ein Coordinator und mehrere Clients befinden. Der Coordinator wird von den Clients als Firewall verwendet. Der Coordinator selbst befindet sich hinter einer Firewall mit statischem NAT. Auf der Firewall sind alle benötigten Regeln zur Umleitung des Traffics eingestellt (s. Einstellungen auf der Firewall überprüfen auf S. 19). Der Remotebenutzer verbindet sich mit der Niederlassung über das Internet (s. Abbildung 2 auf S. 15).

Netzwerkparameter in ViPNet Network Manager einstellen

ViPNet Netzwerk einrichten

Legen Sie die Netzwerkstruktur mit Hilfe des Assistenten **ViPNet Netzwerkaufbau** fest (s. „ViPNet VPN. Benutzerhandbuch“, Kapitel 3, Abschnitt „Erstellen des ViPNet Netzwerks“):

1. Geben Sie die benötigte Anzahl an Coordinatoren und Clients an. Für Verbindungen eines Remotebenutzers zur Firmenniederlassung (s. Abbildung 2 auf S. 15) reicht ein Coordinator aus.
2. Legen Sie den Typ der Verbindungen zwischen ViPNet Netzwerkknoten fest.
3. Wenn nötig, modifizieren Sie die erstellte Struktur und die Verbindungen zwischen den Netzwerkknoten.
4. Wenn Sie die Zugangsparameter zum Coordinator einstellen möchten, wählen Sie als Typ der Verbindung zum Internet **Verbindung über eine Firewall** (s. Abschnitt „Konfiguration des Zugangs zum Coordinator“, Unterabschnitt „Konfiguration des Zugang zum Coordinator, der über eine Firewall mit dem Internet verbunden ist“) und geben die IP-Adresse oder DNS-Namen der Firewall an.

   Wählen Sie die Option **Später im ViPNet Network Manager konfigurieren**, um die Zugangsparameter für den Coordinator später zu konfigurieren.

Hinweis. Mit Hilfe des Assistenten **ViPNet Netzwerkaufbau** können Zugangsparameter nur für den ersten angelegten Coordinator konfiguriert werden (auf diesem Coordinator ist standardmäßig das Manager-Arbeitsplatz – die Arbeitsstation des ViPNet Administrators – registriert). Wenn Zugangsparameter für einen anderen Coordinator konfiguriert werden sollen, verwenden Sie dazu das Hauptfenster von ViPNet Network Manager.

---

5. Definieren Sie die Eigenschaften der Zufallspasswörter für die Benutzer.
6. Deaktivieren Sie auf der letzten Seite des Assistenten die Option **Die Schlüsseldistributionen werden nach dem Beenden des Assistents erstellt** und klicken auf **Fertig**.

ViPNet Netzwerkparameter konfigurieren

Führen Sie die folgenden Schritte aus, um die Parameter der Netzwerkknoten einzustellen:

1 Wählen Sie im Hauptfenster des Programms ViPNet Network Manager im Navigationsbereich denjenigen Coordinator aus, über den Verbindungen zu externen Netzwerkknoten aufgebaut werden sollen. Öffnen Sie die Registerkarte **Zugangsadressen**.

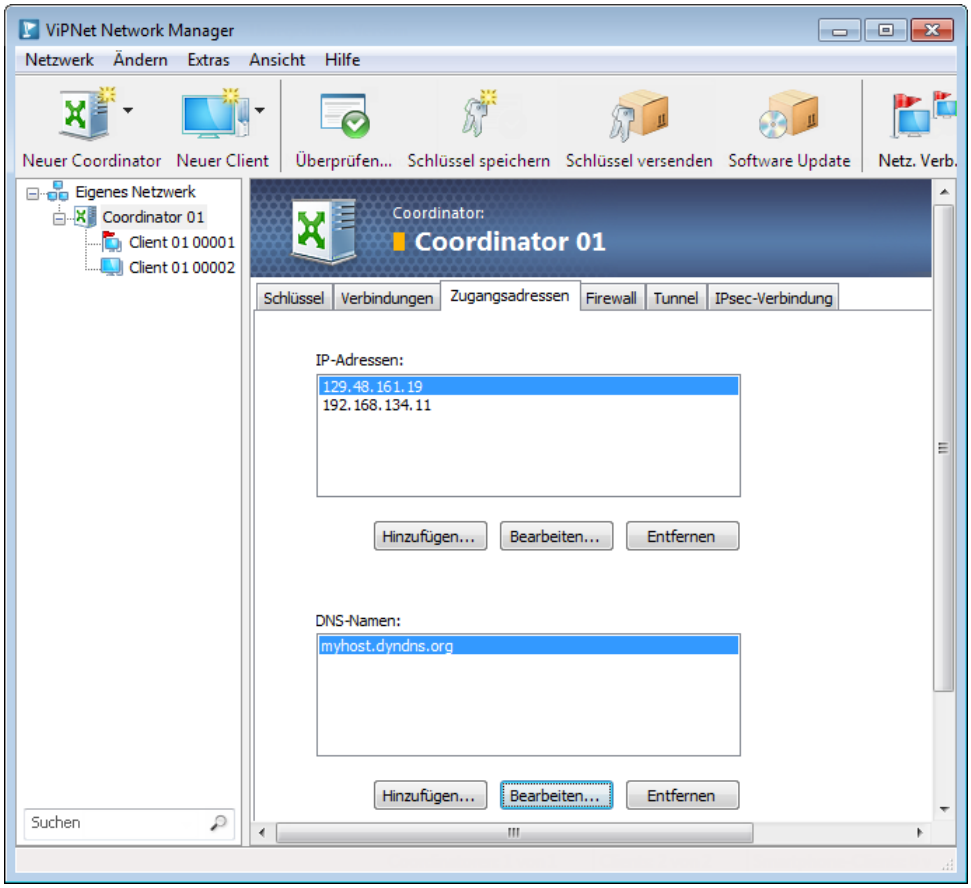

Abbildung 3. IP-Adresse und DNS-Namen des Coordinators definieren

Wenn beim Erstellen der Netzwerkstruktur die Zugangseinstellungen für den Coordinator bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann wird die IP-Adresse des Netzwerkadapters, der an die Firewall angeschlossen ist, in der Liste eingeblendet.

Klicken Sie auf **Hinzufügen**, um die IP-Adresse und DNS-Namen zu definieren. Geben Sie im Fenster **IP-Adresse** oder **DNS-Name** die IP-Adresse oder DNS-Namen des Coordinators ein und klicken auf **OK**.

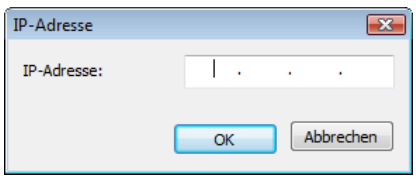

Abbildung 4. IP-Adresse hinzufügen

2 Öffnen Sie die Registerkarte **Firewall**.

Abbildung 5. Firewallparameter konfigurieren

Wenn beim Anlegen des Netzwerks die Zugangsparameter für den Coordinator bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann sind keine weiteren Einstellungen auf der Firewall mehr nötig.

Anderenfalls führen Sie die folgenden Schritte durch:

- Aktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**.
- Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit statischem NAT**.

3 Wählen Sie in der Navigationsleiste den Client aus, der remote arbeiten soll. Öffnen Sie die Registerkarte **Verbindungen** und stellen sicher, dass in der Liste alle Netzwerkknoten aufgeführt sind, mit denen der gegebene Client kommunizieren soll.

4 Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken dann auf **Schlüsseldistributionen speichern**. Kopieren Sie die erstellten Schlüsseldistributionen auf einen abnehmbaren Datenträger. Installieren Sie mit Hilfe dieser Distributionen die ViPNet Schlüssel auf dem Coordinator und auf den Clients.

Einstellungen auf der Firewall überprüfen

Es wird empfohlen, die Konfiguration so vorzunehmen, dass die Firewall (oder ein anderes Gerät, das die Adressenübersetzung durchführt) über eine statische externe IP-Adresse verfügt. Wenn das nicht der Fall ist, verwenden Sie einen dynamischen DNS-Dienst, der die externen dynamischen IP-Adressen der Firewall in einen vordefinierten DNS-Namen umwandelt (dazu kann der Dienst wie www.dynDNS.com verwendet werden).

Auf der Firewall sollten folgende Regeln konfiguriert werden:

1 Definieren Sie einen UDP-Zugangsport, über den verschlüsselter Traffic netzwerkübergreifend ausgetauscht werden soll.

Hinweis. Standardmäßig wird von ViPNet Software der Port 55777 verwendet. Diese Portnummer kann bei Bedarf geändert werden.

---

2 Erstellen Sie eine Regel für die Umleitung des ein- und ausgehenden UDP-Traffics: erlauben Sie beliebigen eingehenden UDP-Traffic, der auf dem definierten Port eintrifft, und leiten diesen zum Coordinator weiter.

Einstellungen auf dem Coordinator überprüfen

Stellen Sie sicher, dass der Coordinator richtig konfiguriert ist. Dazu:

1 Wählen Sie im Hauptfenster von ViPNet Coordinator im Menü **Service** den Eintrag **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.

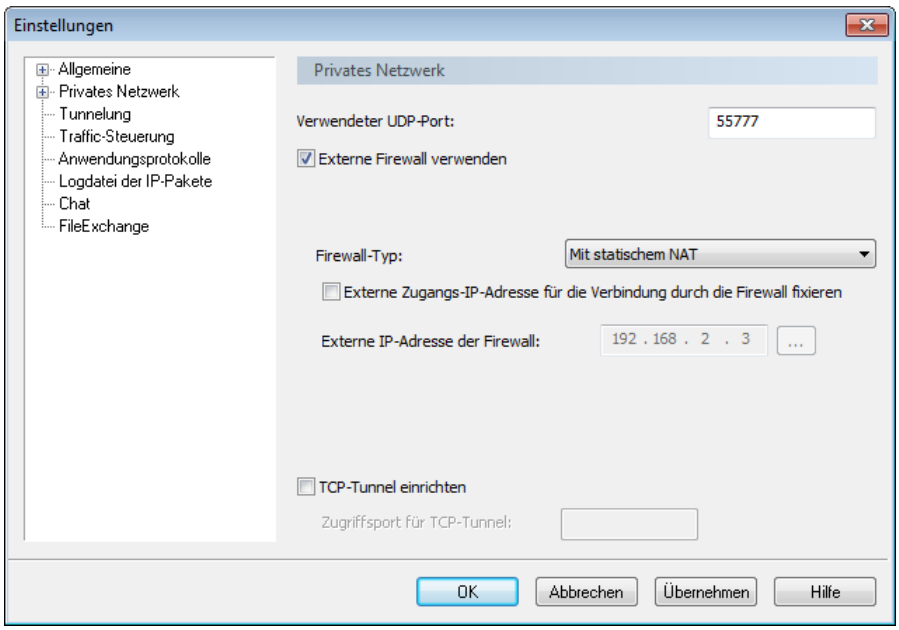

Abbildung 6. Einstellungen auf dem Coordinator überprüfen

2 Stellen Sie sicher, dass das Kontrollkästchen **Externe Firewall verwenden** im Bereich **Privates Netzwerk** aktiviert ist.

3 Stellen Sie sicher, dass der Eintrag **Mit statischem NAT** in der Dropdownliste **Firewall-Typ** ausgewählt ist.

4 Stellen Sie sicher, dass die Portnummer, die auf der Firewall in den Regeln der Trafficumleitung definiert wurde, im Feld **Verwendeter UDP-Port** angegeben ist.

Einstellungen auf den Clients in der Niederlassung überprüfen

Führen Sie die folgenden Schritte durch, um Einstellungen auf Clients, die sich in der Niederlassung befinden, zu überprüfen:

1. Melden Sie sich in Programm ViPNet Client als Administrator an.
2. Wählen Sie im Menü **Service** den Eintrag **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.
3. Stellen Sie im Fenster **Einstellungen** sicher, dass der Coordinator, der sich in der Niederlassung befindet, im Bereich **Privates Netzwerk** als Verbindugsserver ausgewählt ist.

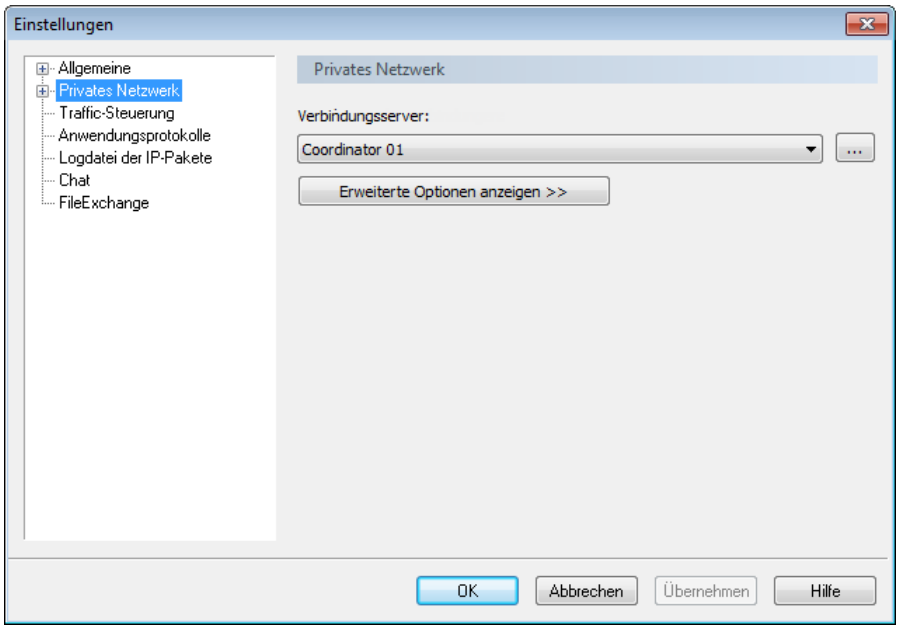

Abbildung 7. Parameter des geschützten Netzwerks

4. Klicken Sie auf **OK**.
5. Wählen Sie in der Navigationsleiste des Hauptfensters von ViPNet Client den Bereich **Privates Netzwerk**.
6. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf den Coordinator, der für den gegebenen Client als Verbindungsserver definiert ist. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
7. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adresse**.

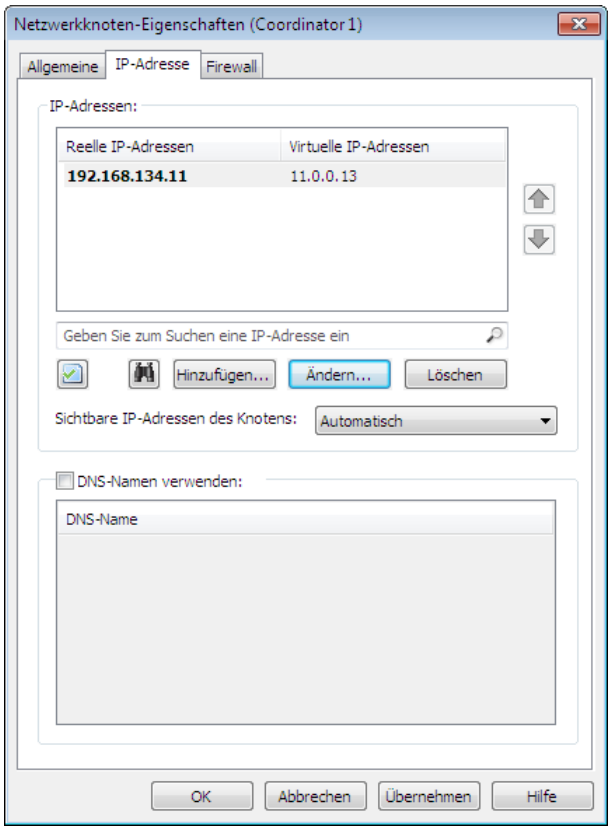

Abbildung 8. IP-Adressen des Coordinators

8 Stellen Sie sicher, dass in der Tabelle **IP-Adresse** in Spalte **Reelle IP-Adressen** die IP-Adresse des Coordinators korrekt definiert ist.

Falls DNS-Namen verwendet werden, stellen Sie sicher, dass das Kontrollkästchen **DNS-Name verwenden** aktiviert ist und in der Liste **DNS-Name** der korrekte DNS-Name des Coordinators angegeben ist.

9 Überprüfen Sie die Verbindung zum Coordinator. Wählen Sie dazu den Coordinator im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

Einstellungen auf den Remote-Clients überprüfen

Führen Sie die folgenden Schritte durch, um die Einstellungen auf einem Remote-Client zu überprüfen:

1. Melden Sie sich in Programm ViPNet Client als Administrator an.
2. Wählen Sie im Menü **Service** den Eintrag **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.
3. Stellen Sie im Fenster **Einstellungen** sicher, dass der Coordinator, der sich in der Niederlassung befindet, im Bereich **Privates Netzwerk** als Verbindungsserver ausgewählt ist.
4. Klicken Sie auf **OK**.
5. Wählen Sie in der Navigationsleiste des Hauptfensters von ViPNet Client den Bereich **Privates Netzwerk**.
6. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf den Coordinator, der für den gegebenen Client als IP-Adressenserver definiert ist. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
7. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Firewall**.

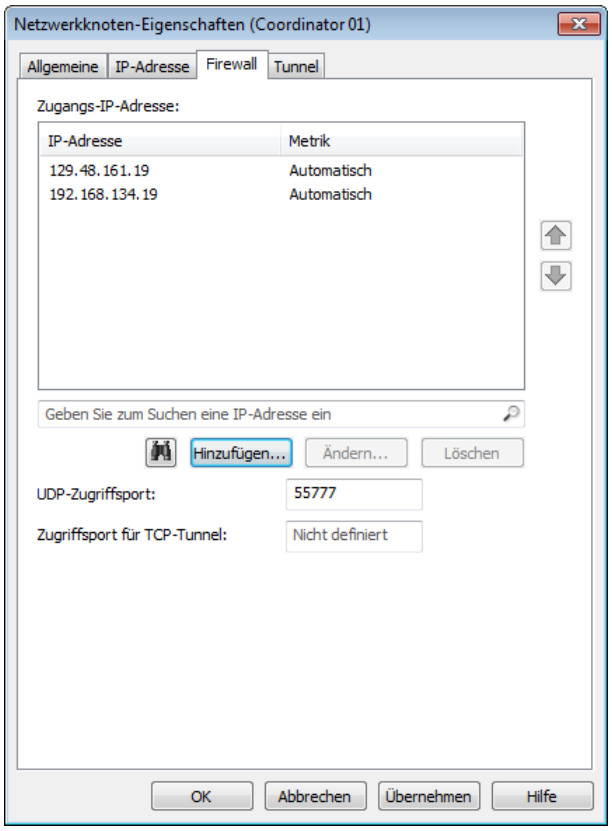

Abbildung 9. Zugangs-IP-Adressen

8 In Tabelle **IP-Adressen** sollte die externe IP-Adresse der Firewall, hinter der sich der Coordinator befindet, aufgelistet sein. Wenn die Firewall über keine statische IP-Adresse verfügt, überprüfen Sie den DNS-Namen der Firewall (Schritt **12**).

9 Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adressen** (s. Abbildung 8 auf S. 22).

10 Stellen Sie sicher, dass in der Tabelle **IP-Adresse** in Spalte **Reelle IP-Adressen** die IP-Adresse des Coordinators korrekt definiert ist.

   Falls DNS-Namen verwendet werden, stellen Sie sicher, dass das Kontrollkästchen **DNS-Name verwenden** aktiviert ist und in der Liste **DNS-Name** der korrekte DNS-Name der Firewall, hinter der sich der Coordinator befindet, angegeben ist.

11 Überprüfen Sie die Verbindung zum Coordinator. Wählen Sie dazu den Coordinator im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen dem Remote-Client und dem Büronetzwerk hergestellt.

2

Verbindungen zwischen zwei Remotebenutzern

Kurze Übersicht 26

Netzwerkparameter in ViPNet Network Manager einstellen 27

Einstellungen auf der Firewall und auf dem Coordinator überprüfen 28

Einstellungen auf den Remote-Clients überprüfen 29

Kurze Übersicht

Dieses Kapitel beschreibt das Schema eines ViPNet VPN-Netzwerks, in welchem zwei entfernte Benutzer Verbindungen zueinander herstellen.

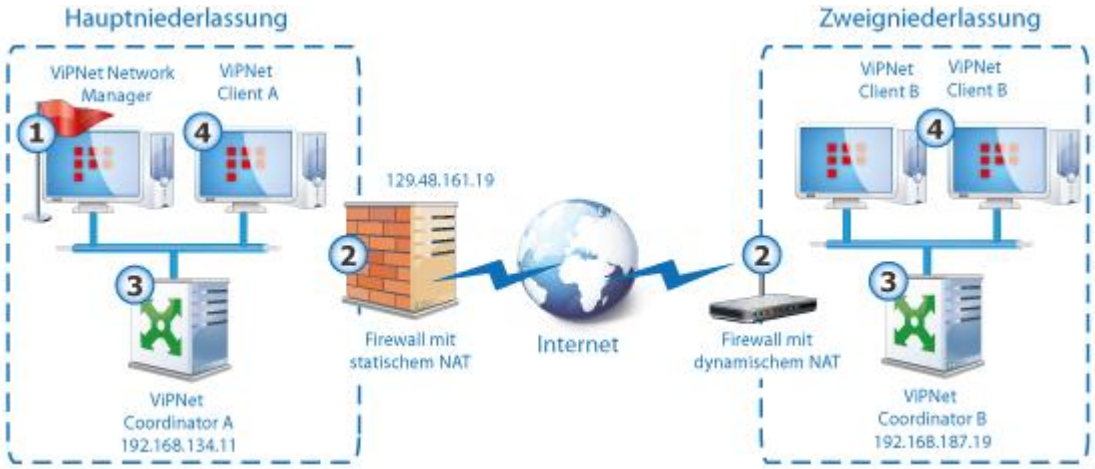

Abbildung 10. Verbindung zwischen zwei Remotebenutzern

Dieses Schema hat dem vorherigen Schema viel gemeinsam (s. Verbindungen zwischen Remotebenutzer und Niederlassung auf S. 14). Nehmen wir an, es befinden sich in der Niederlassung ein Coordinator und mehrere Clients. Der Coordinator befindet sich hinter einer Firewall mit statischem NAT. Auf der Firewall sind alle erforderlichen Regeln zur Traffic-Umleitung konfiguriert (s. Einstellungen auf der Firewall überprüfen auf S. 19). Der Remotebenutzer und der Mitarbeiter, der von zu Hause arbeitet, bauen Verbindungen zueinander und zur Niederlassung über das Internet auf.

Netzwerkparameter in ViPNet Network Manager einstellen

Erstellen Sie zunächst die benötigte ViPNet Netzwerkstruktur wie in Kapitel ViPNet Netzwerk einrichten (auf S. 16) beschrieben ist. Damit die weiter oben vorgegebene Netzwerkstruktur realisiert werden kann (s. Abbildung 10 auf S. 26), sollte ein Coordinator, eine bestimmte Anzahl an Clients für die Arbeit in der Niederlassung sowie zwei zusätzliche Clients für die Remote-Arbeit eingerichtet werden.

Führen Sie im Programm ViPNet Network Manager die folgenden Schritte durch, um die Parameter des ViPNet Netzwerks einzustellen:

1. Wählen Sie in der Navigationsleiste von ViPNet Network Manager den Coordinator aus, über welchen Verbindungen zu externen Netzwerkknoten aufgebaut werden sollen. Öffnen Sie die Registerkarte **Zugangsadressen** (s. Abbildung 3 auf S. 17).

   Wenn beim Anlegen des Netzwerks die Zugangsparameter für den Coordinator bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann wird die IP-Adresse des Netzwerkadapters automatisch in der Liste eingeblendet. Wenn die IP-Adresse nicht festgelegt wurde, klicken Sie in der Gruppe **IP-Adressen** auf **Hinzufügen**. Geben Sie im Fenster **IP-Adresse** die IP-Adresse des Coordinators ein und klicken auf **OK**.

   Wenn die Firewall des Coordinators über DNS-Namen erreichbar ist (z.B., dznDNS wird verwendet), in der Gruppe **DNS-Namen** klicken Sie auf **Hinzufügen** un geben den Namen des Coordinators ein.

2. Öffnen Sie die Registerkarte **Firewall** (s. Abbildung 5 auf S. 18).

   Wenn beim Anlegen des Netzwerks die Zugangsparameter für den Coordinator bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann sind keine weiteren Einstellungen auf der Firewall mehr nötig.

   Anderenfalls führen Sie die folgenden Schritte durch:

   - Aktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**.
   - Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit statischem NAT**.

3. Wählen Sie in der Navigationsleiste den Client aus. Öffnen Sie die Registerkarte **Verbindungen** und stellen Sie sicher, dass alle Netzwerkknoten, mit denen der gegebene Client kommunizieren soll, in der Liste aufgeführt sind.

4. Wiederholen Sie den Schritt **3**, um die Konfiguration des zweiten Remote-Clients durchzuführen.

5. Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken Sie dann auf **Schlüsseldistributionen speichern**. Kopieren Sie die erstellten Schlüsseldistributionen auf einen abnehmbaren Datenträger. Installieren Sie mit Hilfe dieser Distributionen die ViPNet Software auf dem Coordinator und auf den Clients.

Einstellungen auf der Firewall und auf dem Coordinator überprüfen

Stellen Sie sicher, dass die Firewall über eine statische externe IP-Adresse oder über einen DNS-Namen, der mit Hilfe des dynamischen Namensdienstes registriert wurde, verfügt. Ebenso sollten auf der Firewall alle erforderlichen Regeln zur Traffic-Umleitung konfiguriert sein (s. Einstellungen auf der Firewall überprüfen auf S. 19).

Überprüfen Sie auf dem Computer, der als Coordinator auftritt, die Einstellungen im Programm ViPNet Monitor (s. Einstellungen auf dem Coordinator überprüfen auf S. 20).

Einstellungen auf den Remote-Clients überprüfen

Hinweis. Alle Remote-Clients im ViPNet Netzwerk sollten über die gleichen, weiter unten aufgeführten Einstellungen verfügen.

Führen Sie die folgenden Schritte durch, um die Einstellungen auf einem Remote-Client zu überprüfen:

1. Melden Sie sich in Programm ViPNet Client als Administrator an.
2. Wählen Sie im Menü **Service** den Eintrag **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.
3. Stellen Sie im Fenster **Einstellungen** sicher, dass der Coordinator, der sich in der Niederlassung befindet, im Bereich **Privates Netzwerk** als Verbindungsserver ausgewählt ist.
4. Klicken Sie auf **OK**.
5. Wählen Sie in der Navigationsleiste des Hauptfensters von ViPNet Client den Bereich **Privates Netzwerk**.
6. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf den Coordinator, der für den gegebenen Client als IP-Adressenserver definiert ist. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
7. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Firewall** (s. Abbildung 9 auf S. 23).
8. Stellen Sie sicher, dass das Kontrollkästchen **Firewall-Einstellungen verwenden** aktiviert ist. In Tabelle **IP-Adressen** sollte die externe IP-Adresse der Firewall, hinter der sich der Coordinator befindet, angegeben sein. Wenn die Firewall über keine statische IP-Adresse verfügt, überprüfen Sie den DNS-Namen der Firewall (Schritt **12**).
9. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adressen** (s. Abbildung 8 auf S. 22).
10. Stellen Sie sicher, dass die IP-Adresse des Coordinators in der Tabelle **IP-Adresse** in Spalte **Reelle IP-Adressen** korrekt definiert ist.

    Falls DNS-Namen verwendet werden, stellen Sie sicher, dass das Kontrollkästchen **DNS-Name verwenden** aktiviert ist und der korrekte DNS-Name der Firewall, hinter der sich der Coordinator befindet, in der Liste **DNS-Name** angegeben ist.
11. Stellen Sie sicher, dass der zweite Remote-Benutzer und alle anderen ViPNet Netzwerkknoten, mit denen der gegebene Client kommunizieren soll, im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten aufgelistet sind.

12 Überprüfen Sie die Verbindung zum Coordinator und zum zweiten Remote-Client. Wählen Sie dazu im Bereich **Privates Netzwerk** den benötigten Netzwerkknoten aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen den Remote-Clients und dem Niederlassungsnetzwerk hergestellt.

3

Verbindungen zwischen zwei Niederlassungen

Kurze Übersicht 32

Netzwerkparameter in ViPNet Network Manager einstellen 33

Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen 35

Einstellungen der Clients beider Niederlassungen überprüfen 37

Kurze Übersicht

Dieses Kapitel beschreibt das Schema eines ViPNet VPN-Netzwerks, in welchem geschützte Verbindungen zwischen der Firmenniederlassung und der Zweigniederlassung hergestellt werden.

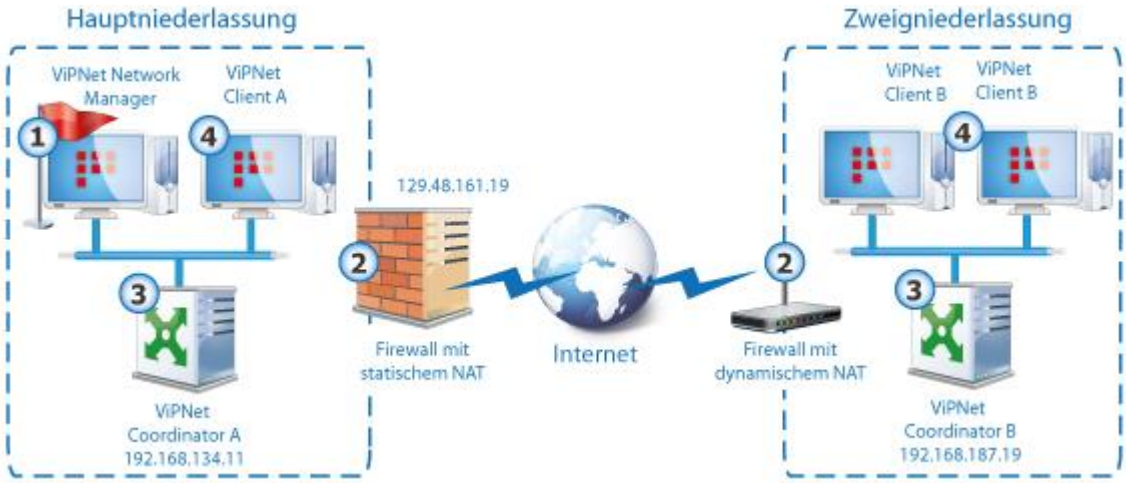

Abbildung 11. Verbindung zwischen zwei Niederlassungen

Nehmen wir an, innerhalb der Organisation gibt es eine Hauptniederlassung und eine Zweigniederlassung. Computer, die sich in der Hauptniederlassung und in der Zweigniederlassung befinden, sind in einem firmenübergreifenden ViPNet Netzwerk zusammengefasst. Coordinator A, der sich in der Hauptniederlassung befindet, und Coordinator B, der in der Zweigniederlassung aufgestellt ist, bauen abgesicherte Verbindungen zueinander über das Internet auf. Coordinator A befindet sich hinter einer Firewall, auf der eine statische Regel zur Traffic-Umleitung eingestellt ist, die den Austausch verschlüsselter Daten zwischen den Knoten ermöglicht. Coordinator B befindet sich hinter einer Firewall, auf der keine speziellen Einstellungen für den Austausch verschlüsselter Daten vorgenommen wurden. Die Clients der Hauptniederlassung (einer der Clients dient als Network Control Center) verwenden Coordinator A als Firewall. Die Clients der Zweigniederlassung verwenden Coordinator B als Firewall.

Nur ein Bereich des Netzwerks (in unserem Beispiel die Hauptniederlassung) sollte über eine externe statische IP-Adresse oder über einen DNS-Namen von außen ansprechbar sein (s. Bevor Sie mit der Arbeit beginnen auf S. 12).

Netzwerkparameter in ViPNet Network Manager einstellen

Erstellen Sie zunächst die benötigte ViPNet Netzwerkstruktur, wie in Kapitel ViPNet Netzwerk einrichten (auf S. 16) beschrieben. Damit die oben vorgegebene Netzwerkstruktur realisiert werden kann (s. Abbildung 11 auf S. 32), sollten zwei Coordinatoren eingerichtet werden. Auf Coordinator A sollten Clients registriert werden, die in der Hauptniederlassung arbeiten werden. Auf Coordinator B sollten Clients registriert werden, die in der Zweigniederlassung zum Einsatz kommen.

Führen Sie im Programm ViPNet Network Manager für jeden Coordinator die folgenden Einstellungen durch:

1 Wählen Sie im Hauptfenster des Programms ViPNet Network Manager in der Navigationsleiste Coordinator A aus und öffnen die Registerkarte **Zugangsadressen**.

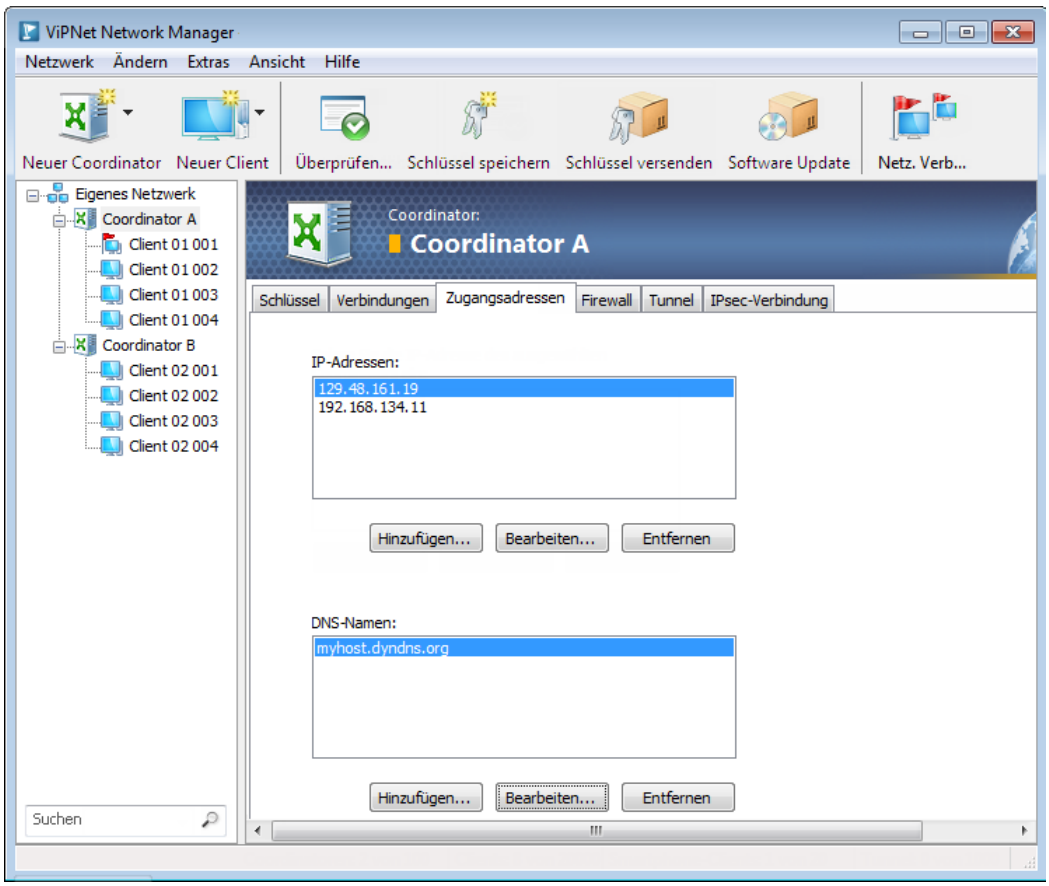

Abbildung 12. IP-Adresse und DNS-Namen des Coordinators festlegen

Wenn beim Anlegen des Netzwerks die Zugangsparameter für den Coordinator A bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann wird die IP-Adresse des Netzwerkadapters,

der Coordinator A (in unserem Beispiel – 192.168.134.11) mit der Firewall verbindet, automatisch in der Liste eingeblendet. Klicken Sie in der Gruppe **IP-Adressen** auf **Hinzufügen**, um eine IP-Adresse anzugeben. Geben Sie im Fenster **IP-Adresse** die IP-Adresse des Coordinators A (in unserem Fall 192.168.134.11) ein und klicken Sie auf **OK**.

Wenn der Zugriff auf Coordinator A aus dem Internet über einen DNS-Namen erfolgt (z.B. mit Hilfe von dynDNS), dann klicken Sie in der Gruppe **DNS-Namen** auf **Hinzufügen** und gebe Sie den Namen des Coordinators an.

2 Öffnen Sie die Registerkarte **Firewall**.

Wenn beim Anlegen des Netzwerks die Zugangsparameter für Coordinator A bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann sind keine weiteren Einstellungen auf der Firewall mehr nötig.

Anderenfalls führen Sie die folgenden Schritte durch:

- Aktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**.
- Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit statischem NAT**.

3 Wählen Sie im Hauptfenster des Programms ViPNet Network Manager in der Navigationsleiste Coordinator B aus, öffnen Sie die Registerkarte **IP-Adressen** und klicken auf **Hinzufügen**. Geben Sie im Fenster **IP-Adresse** die lokale IP-Adresse von Coordinator B ein (in unserem Fall 192.168.187.19) und klicken auf **OK**.

4 Öffnen Sie die Registerkarte **Firewall**:

- Aktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**.
- Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit dynamischem NAT**.
- Wählen Sie in der Dropdownliste **Coordinator für eingehende Verbindungen** den Eintrag `Coordinator A`.
- Stellen Sie sicher, dass das Kontrollkästchen **Jede Verbindung mit externen Netzwerkknoten über den Coordinator umleiten** deaktiviert ist.

5 Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken dann auf **Schlüsseldistributionen speichern**. Kopieren Sie die erstellten Schlüsseldistributionen auf einen abnehmbaren Datenträger. Installieren Sie mit Hilfe dieser Distributionen die ViPNet Software auf dem Coordinator und auf den Clients.

Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen

Die Firewall der Hauptniederlassung sollte über eine statische externe IP-Adresse oder über einen DNS-Namen, der mit Hilfe des dynamischen Namensdienstes registriert wurde, erreichbar sein. Auf dieser Firewall sollte eine Regel der Portweiterleitung (s. Einstellungen auf der Firewall überprüfen auf S. 19) an die lokale IP-Adresse des Coordinators A eingerichtet sein (UDP 55777). Auf der Firewall der Zweigniederlassung müssen keine weiteren Einstellungen durchgeführt werden.

Führen Sie auf jedem Coordinator die folgenden Schritte durch, um sicherzustellen, dass beide Coordinatoren richtig konfiguriert sind:

1. Wählen Sie im Hauptfenster von ViPNet Coordinator im Menü **Service** den Eintrag **Anwendungseinstellungen**.
2. Stellen Sie sicher, dass das Kontrollkästchen **Externe Firewall verwenden** im Bereich **Privates Netzwerk** aktiviert ist.
3. Stellen Sie sicher, dass der Wert **Mit statischem NAT** auf Coordinator A und der Wert **Mit dynamischem NAT** auf Coordinator B in der Dropdownliste **Firewall-Typ** ausgewählt ist.
4. Stellen Sie sicher, dass die Portnummer, die auf der Firewall in den Regeln der Portweiterleitung festgelegt wurde, auf Coordinator A im Feld **Verwendeter UDP-Port** angegeben ist.
5. Stellen Sie sicher, dass Coordinator A auf Coordinator B in der Liste **Verbindungsserver** ausgewählt ist.
6. Wählen Sie auf Coordinator B in der Navigationsleiste des Hauptfensters von ViPNet Coordinator den Bereich **Privates Netzwerk**.
7. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf Coordinator A. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
8. Wenn Coordinator A über eine statische externe IP-Adresse erreichbar ist, dann führen Sie die folgenden Schritte durch:

   8.1 Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Firewall** (s. Abbildung 9 auf S. 23).

   8.2 Stellen Sie sicher, dass das Kontrollkästchen **Firewall-Einstellungen verwenden** aktiviert ist. In Tabelle **IP-Adressen** sollte die statische externe IP-Adresse der Firewall, hinter der sich der Coordinator der anderen Niederlassung befindet, aufgelistet sein (in unserem Fall 129.48.161.19).
9. Wenn die Firewall der Hauptniederlassung über keine statische externe IP-Adresse verfügt, sollten Sie sicherstellen, dass der DNS-Name dieser Firewall richtig angegeben ist.

Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adresse** (s. Abbildung 8 auf S. 22). Stellen Sie sicher, dass das Kontrollkästchen **DNS-Name verwenden** aktiviert und in der Liste **DNS-Name** der korrekte DNS-Name der Firewall, hinter der sich der Coordinator der anderen Niederlassung befindet, angegeben ist.

10 Überprüfen Sie auf Coordinator B die Verbindung zu Coordinator A. Wählen Sie ihn dazu im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen den Coordinatoren der Hauptniederlassung und der Zweigniederlassung hergestellt.

Einstellungen der Clients beider Niederlassungen überprüfen

Hinweis. Die Überprüfung der Korrektheit von Einstellungen sollte auf allen Clients der Hauptniederlassung und der Zweigniederlassung in Übereinstimmung mit den weiter unten aufgeführten Anweisungen durchgeführt werden.

Führen Sie die folgenden Schritte durch, um die Einstellungen auf den Clients zu überprüfen:

1. Melden Sie sich in Programm ViPNet Client Monitor als Administrator an.
2. Wählen Sie im Menü **Service** den Eintrag **Anwendungseinstellungen**. Es wird das Fenster **Einstellungen** geöffnet.
3. Stellen Sie im Fenster **Einstellungen** sicher, dass der Coordinator, der sich in der gleichen Niederlassung befindet, im Bereich **Privates Netzwerk** (s. Abbildung 7 auf S. 21) als Verbindungsserver ausgewählt ist.
4. Klicken Sie auf **OK**.
5. Wählen Sie in der Navigationsleiste des Hauptfensters von ViPNet Client den Bereich **Privates Netzwerk**.
6. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf den Coordinator, der als IP-Adressenserver für den gegebenen Client definiert ist. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
7. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adressen** (s. Abbildung 8 auf S. 22).
8. Stellen Sie sicher, dass in der Tabelle **IP-Adresse** in Spalte **Reelle IP-Adressen** die korrekte IP-Adresse des Coordinators definiert ist (in der Hauptniederlassung – 192.168.134.11, in der Zweigniederlassung – 192.168.87.19).
9. Überprüfen Sie die Verbindung zum Coordinator der Niederlassung, in welcher sich der betroffene Client befindet. Wählen Sie ihn dazu im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.
10. Überprüfen Sie die Verbindung zu einem beliebigen ViPNet Netzwerkknoten in der anderen Niederlassung.

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen der Hauptniederlassung und der Zweigniederlassung hergestellt. Wenn keine Verbindung aufgebaut werden konnte, kann die Ursache in der Inkompatibilität der Softwareversionen oder in den Einstellungen der Firewall liegen. Wenden Sie sich an den technischen Support der Infotecs GmbH.

4

Verbindungen zwischen zwei Niederlassungen mit Hilfe der Tunnelung

Kurze Übersicht 39

Netzwerkparameter in ViPNet Network Manager einstellen 40

Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen 43

Routing-Einstellungen der getunnelten Knoten überprüfen 46

Einstellungen auf Remote-Clients überprüfen 48

Kurze Übersicht

Dieses Kapitel beschreibt das Schema eines ViPNet VPN-Netzwerks, in dem geschützte Verbindungen zwischen den Computern der Haupt- und der Zweigniederlassung mit Hilfe der Tunnelung aufgebaut werden.

Die Tunnelung ist ein Verfahren zum Schutz des Traffics, der über offene (ungeschützte) Verbindungskanäle übertragen wird. Zwischen dem getunnelten Knoten und dem Coordinator werden die IP-Pakete offen übertragen. Zwischen dem Coordinator und anderen ViPNet Netzwerkknoten werden die Pakete verschlüsselt übertragen.

Ein getunnelter Knoten ist ein Netzwerkgerät, auf dem keine ViPNet Software installiert ist. Dieses Gerät sollte von außen über einen geschützten Verbindungskanal unter Beteiligung des Coordinators erreichbar sein. Es können PC- oder Apple-Computer, Netzwerkdrucker, NAS-Geräte, VoIP-Geräte, usw. getunnelt werden.

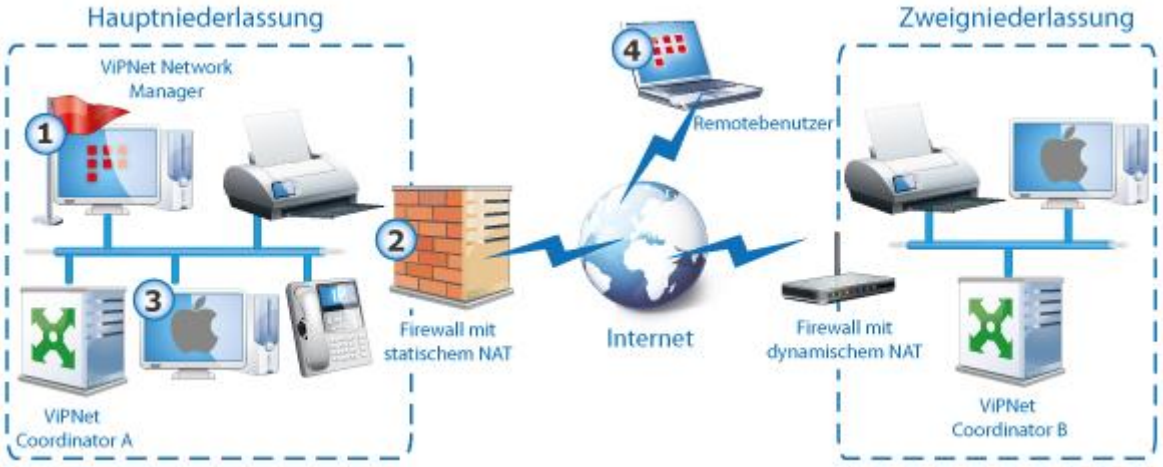

Abbildung 13. Verbindungen zwischen zwei Niederlassungen mit Hilfe der Tunnelung

Nehmen wir an, innerhalb der Organisation gibt es eine Hauptniederlassung und eine Zweifniederlassung. Das ViPNet Firmennetzwerk umfasst zwei Coordinatoren, ein Manager-Arbeitsplatz und einen entfernten ViPNet Netzwerkknoten. Coordinator A, der sich in der Hauptniederlassung befindet, und Coordinator B, der sich in der Zweigniederlassung befindet, bauen eine geschützte Verbindung über das Internet auf. Coordinator A befindet sich hinter einer Firewall, auf der statische Regeln zur Traffic-Umleitung eingestellt sind, um den Austausch geschützter Daten zu ermöglichen. Coordinator B befindet sich hinter einer Firewall, auf der keine zusätzlichen Einstellungen für den Austausch verschlüsselter Daten vorgenommen wurden. Von Coordinator A werden mehrere offene (ohne ViPNet Software) Computer und Geräte in der Hauptniederlassung getunnelt. Von Coordinator B werden mehrere offene Computer und Netzwerkgeräte in der Zweigniederlassung getunnelt. Ein entfernter ViPNet Benutzer stellt Verbindungen zu getunnelten Knoten in beiden Niederlassungen her.

Netzwerkparameter in ViPNet Network Manager einstellen

Netzwerkparameter in ViPNet Network Manager einstellen wie in Kapitel ViPNet Netzwerk einrichten (auf S. 16) beschrieben. Damit die oben vorgegebene Netzwerkstruktur realisiert werden kann (s. Abbildung 13 auf S. 39), sollten zwei Coordinatoren und zwei Clients eingerichtet werden (Manager-Arbeitsplatz und ViPNet Remoteknoten).

Hinweis. Bei Bedarf können zusätzliche Clients für die Arbeit in einem der Büros oder für entfernte Arbeit eingerichtet werden.

Führen Sie im Programm ViPNet Network Manager für jeden Coordinator die folgenden Einstellungen durch:

1 Wählen Sie im Hauptfenster des Programms ViPNet Network Manager in der Navigationsleiste den Coordinator A und öffnen die Registerkarte **Zugangsadressen** (s. Abbildung 12 auf S. 33).

Wenn beim Anlegen des Netzwerks die Zugangsparameter für Coordinator A bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann wird die IP-Adresse des Netzwerkadapters, der Coordinator A mit der Firewall verbindet, automatisch in der Liste eingeblendet. Klicken Sie in der Gruppe **IP-Adresse** auf **Hinzufügen**, um eine IP-Adresse anzugeben. Geben Sie im Fenster **IP-Adresse** die lokale IP-Adresse des Coordinators ein und klicken auf **OK**.

Wenn der Zugriff auf Coordinator A aus dem Internet über einen DNS-Namen erfolgt (z.B. mit Hilfe von dynDNS), klicken Sie in der Gruppe **IP-Adresse** auf **Hinzufügen** und geben DNS-Namen des Coordinators ein.

2 Öffnen Sie die Registerkarte **Firewall** (s. Abbildung 5 auf S. 18).

Wenn beim Anlegen des Netzwerks die Zugangsparameter für Coordinator A bereits definiert wurden (s. ViPNet Netzwerk einrichten auf S. 16), dann sind keine weiteren Einstellungen auf der Firewall mehr nötig.

Anderenfalls führen Sie die folgenden Schritte durch:

- Aktivieren Sie das Kontrollkätschen **Externe Firewall verwenden**.
- Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit statischem NAT**.

3 Wählen Sie im Hauptfenster des Programms ViPNet Network Manager in der Navigationsleiste Coordinator B aus, öffnen die Registerkarte **Zugangsadressen** und klicken in der Gruppe **IP-Adresse** auf **Hinzufügen**. Geben Sie im Fenster **IP-Adresse** die lokale IP-Adresse von Coordinator B ein und klicken auf **OK**.

4 Öffnen Sie die Registerkarte **Firewall**:

- Aktivieren Sie das Kontrollkätschen **Externe Firewall verwenden**.
- Wählen Sie in der Dropdownliste **Firewall-Typ** den Eintrag **Mit dynamischem NAT**.
- Wählen Sie in der Dropdownliste **Coordinator für eingehende Verbindungen** den Eintrag `Coordinator A`.
- Stellen Sie sicher, dass das Kontrollkästchen **Jede Verbindung mit externen Netzwerkknoten über den Coordinator umleiten** deaktiviert ist.

Nehmen Sie für beide Coordinatoren die folgenden Einstellungen vor:

5 Öffnen Sie die Registerkarte **Tunnel**.

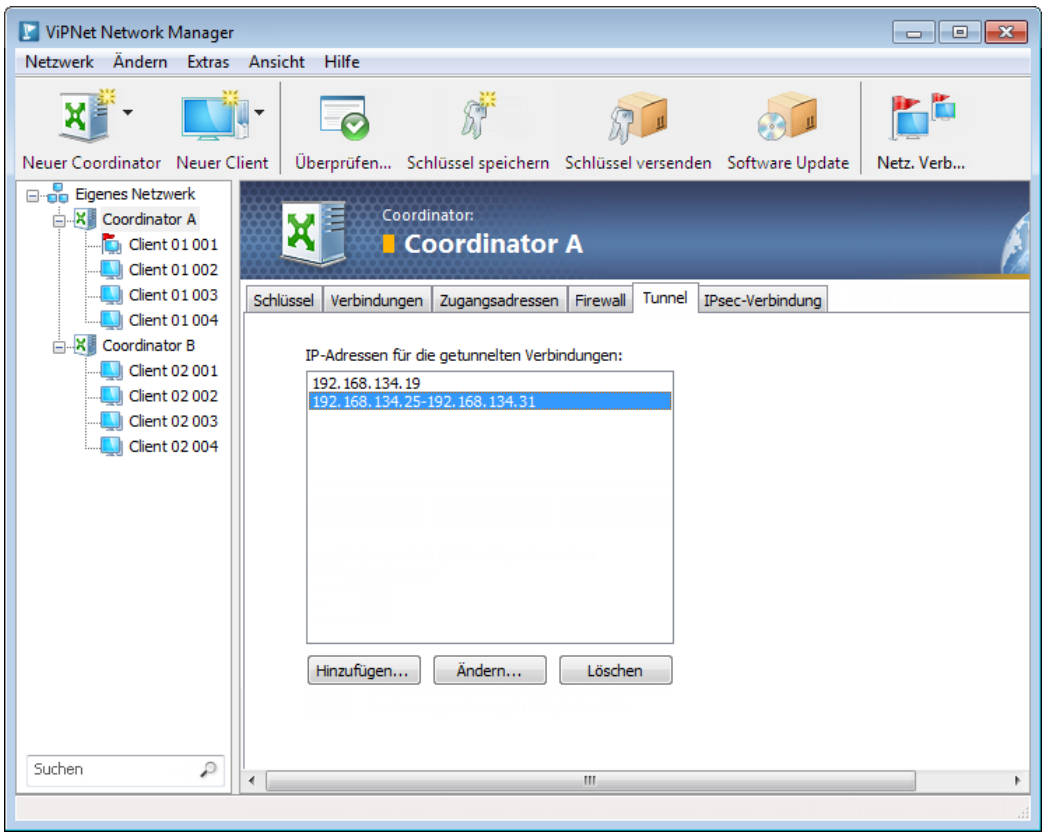

Abbildung 14. IP-Adressen getunnelter Verbindungen eingeben

Geben Sie in der Registerkarte **Tunnel** die IP-Adressen der Computer und Netzwerkgeräte an, die vom gegebenen Coordinator getunnelt werden sollen. Der Coordinator und die von ihm getunnelten Netzwerkobjekte sollten sich im gleichen Netzwerksegment befinden.

Hinweis. Empfehlungen für den Fall, dass sich der Coordinator und die getunnelten Knoten in unterschiedlichen Netzwerksegmenten befinden, sind im Dokument „Gängige Szenarien der Administration von ViPNet VPN. Anhang zum Benutzerhandbuch“ (Kapitel „Tunnelung von Knoten, die sich nicht im Subnetz des tunnelenden Coordinators befinden“) enthalten.

Führen Sie die folgenden Schritte durch, um eine IP-Adresse anzugeben:

- Klicken Sie auf **Hinzufügen**. Es wird das Fenster **IP-Adresse oder Bereich** geöffnet.

- Wenn nur eine getunnelte IP-Adresse definiert werden soll, dann wählen Sie die Option **IP-Adresse** und geben im Eingabefeld die benötigte Adresse ein.
- Wenn ein Bereich getunnelter IP-Adressen definiert werden soll, dann wählen Sie die Option **Bereich** und geben im Eingabefeld die Anfangs- und die Endadresse des Bereichs ein.
- Klicken Sie auf **OK**.

Führen Sie die folgenden Schritte durch, um den Remote-Client zu konfigurieren:

1. Wählen Sie in der Navigationsleiste den Client aus, der remote arbeiten soll.
2. Öffnen Sie die Registerkarte **Verbindungen** und stellen sicher, dass in der Liste alle Netzwerkknoten aufgeführt sind, mit denen der gegebene Client kommunizieren soll. Verbindungen zu getunnelten Netzwerkobjekten sind standardmäßig immer erlaubt. Diese Objekte werden nicht in der Liste aufgeführt.

Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken dann auf **Schlüsseldistributionen speichern**. Kopieren Sie die erstellten Schlüsseldistributionen auf einen abnehmbaren Datenträger. Installieren Sie mit Hilfe dieser Distributionen die ViPNet Schlüssel auf dem Coordinator und auf den Clients.

Einstellungen auf Firewalls und Coordinatoren beider Niederlassungen überprüfen

Die Firewall der Hauptniederlassung sollte über eine statische externe IP-Adresse oder über einen DNS-Namen, der mit Hilfe des dynamischen Namensdienstes registriert wurde, erreichbar sein. Auf dieser Firewall sollte eine Regel der Traffic-Umleitung (s. Einstellungen auf der Firewall überprüfen auf S. 19) an die lokale IP-Adresse des Coordinators A eingerichtet sein (UDP 55777). Auf der Firewall der Zweigniederlassung müssen keine weiteren Einstellungen durchgeführt werden.

Führen Sie auf jedem Coordinator die folgenden Schritte durch, um sicherzustellen, dass beide Coordinatoren richtig konfiguriert sind:

1. Wählen Sie im Hauptfenster von ViPNet Coordinator im Menü **Service** den Eintrag **Anwendungseinstellungen**.
2. Stellen Sie sicher, dass im Bereich **Privates Netzwerk** das Kontrollkästchen **Externe Firewall verwenden** aktiviert ist.
3. Stellen Sie sicher, dass der Wert **Mit statischem NAT** auf Coordinator A in der Liste **Firewall-Typ** und der Wert **Mit dynamischem NAT** auf Coordinator B ausgewählt ist.
4. Stellen Sie sicher, dass die Portnummer, die auf der Firewall in den Regeln der Traffic-Umleitung festgelegt wurde, auf Coordinator A im Feld **Verwendeter UDP-Port** angegeben ist.
5. Stellen Sie sicher, dass Coordinator A auf Coordinator B in der Liste **Verbindungsserver** ausgewählt ist.
6. Gehen Sie bei beiden Coordinatoren wie folgt vor: wählen Sie im Fenster **Einstellungen** den Bereich **Tunnelung**.

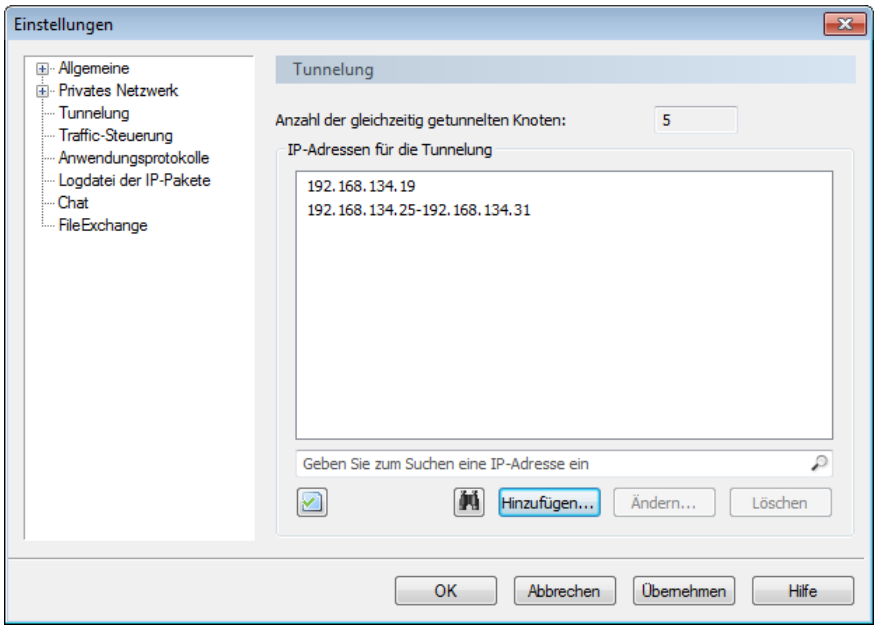

Abbildung 15. IP-Adressen für die Tunnelung überprüfen

Überprüfen Sie die IP-Adressen getunnelter Netzwerkknoten. Alle Knoten, die vom gegebenen Coordinator getunnelt werden, sollten sich mit diesem Coordinator im gleichen Subnetz befinden.

7 Wählen Sie auf Coordinator B in der Navigationsleiste des Hauptfensters von ViPNet Coordinator den Bereich **Privates Netzwerk**.

8 Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf Coordinator A. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.

9 Wenn Coordinator A über eine statische externe IP-Adresse erreichbar ist, dann führen Sie die folgenden Schritte durch:

- Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Firewall** (s. Abbildung 9 auf S. 23).
- Stellen Sie sicher, dass die statische externe IP-Adresse der Firewall in Tabelle **IP-Adressen** aufgelistet ist.

10 Wenn die Firewall der Hauptniederlassung über keine statische externe IP-Adresse verfügt, sollten Sie sicherstellen, dass der DNS-Name dieser Firewall richtig angegeben ist.

Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adressen** (s. Abbildung 8 auf S. 22). Stellen Sie sicher, dass das Kontrollkästchen **DNS-Name verwenden** aktiviert und in der Liste **DNS-Name** der korrekte DNS-Name der Firewall, hinter der sich der Coordinator der anderen Niederlassung befindet, angegeben ist.

11 Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Tunnel**.

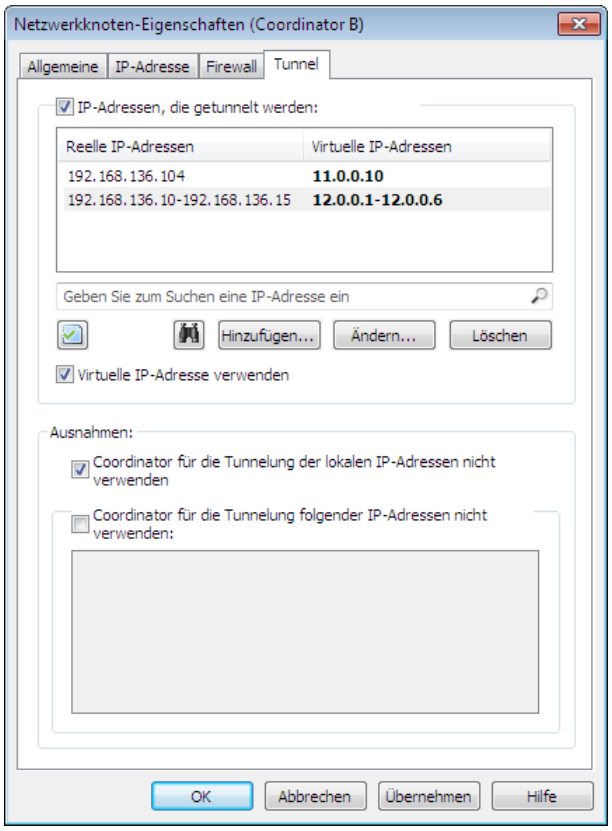

Abbildung 16. IP-Adressen, die vom anderen Coordinator getunnelt werden, überprüfen

Stellen Sie sicher, dass das Kontrollkästchen **IP-Adressen zur Tunnelung verwenden** auf der Registerkarte **Tunnel** aktiviert ist und alle IP-Adressen, die vom anderen Coordinator getunnelt werden, aufgelistet sind.

Wenn im Netzwerk der Haupt- und der Zweigniederlassung die gleichen IP-Adressen verwendet werden, dann aktivieren Sie das Kontrollkästchen **Virtuelle IP-Adressen verwenden**. Diese Option dient dazu, IP-Adressenkonflikte zu vermeiden.

12 Überprüfen Sie auf Coordinator B die Verbindung zu Coordinator A. Wählen Sie dazu den Coordinator im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen den Coordinatoren der Hauptniederlassung und der Zweigniederlassung hergestellt.

Routing-Einstellungen der getunnelten Knoten überprüfen

Es wird empfohlen, die Konfiguration so vorzunehmen, dass jeder getunnelte Netzwerkknoten seinen tunnelenden Coordinator als Standardgateway verwendet. In diesem Fall werden keine weiteren Einstellungen benötigt.

Bei Netzwerkknoten, für die der Coordinator nicht als Standardgateway verwendet werden kann, sollten statische Routen definiert werden, um den für die Tunnelung bestimmten Traffic über den Coordinator zur anderen Niederlassung zu leiten.

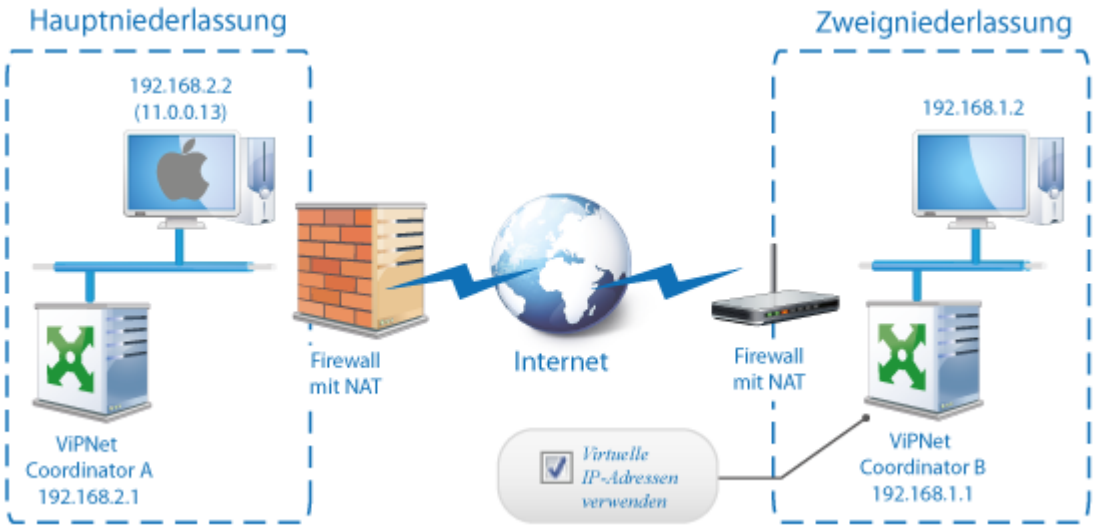

Abbildung 17. Virtuelle IP-Adresse bestimmen

Geben Sie in der Befehlszeile von Windows den folgenden Befehl ein, um eine statische Route zu definieren:

```
route add <destination IP> mask <subnet mask> <gateway> -p,
```

wo:

`<destination IP>` die virtuelle IP-Adresse des Zielsubnetzes.

`<subnet mask>` die Subnetzmaske.

`<gateway>` die lokale IP-Adresse des Coordinators und

`-p` ein Parameter ist, Geben Sie in der Befehlszeile von Windows den folgenden Befehl ein, um eine statische Route zu definieren:

Wenn Sie die IP-Adresse des Zielsubnetzes erfahren möchten:

1. Öffnen Sie auf dem Coordinator, der sich im lokalen Netzwerk des getunnelten Knotens befindet, im Hauptfenster des Programms ViPNet Coordinator den Bereich **Privates Netzwerk**.
2. Doppelklicken Sie in der Liste der ViPNet Netzwerkknoten auf den Coordinator der anderen Niederlassung. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.

3 Öffnen Sie die Registerkarte **Tunnel** und stellen sicher, dass das Kontrollkästchen **Virtuelle IP-Adressen verwenden** aktiviert ist. Netzwerkadressen, die in der Spalte **Virtuelle IP-Adressen** angezeigt werden, sollten bei der Konfiguration von statischen Routen verwendet werden (in unserem Fall handelt es sich um Netzwerk 11).

Es soll zum Beispiel eine Verbindung zwischen den getunnelten Computern, die sich in der Haupt- und in der Zweigniederlassung befinden, hergestellt werden. Auf dem Coordinator der Zweigniederlassung besitzen die getunnelten Computer der Hauptniederlassung virtuelle IP-Adressen aus dem Netzwerk 11.0.0.0 (s. Abbildung 17 auf S. 46). Die lokale IP-Adresse des Coordinators der Zweigniederlassung ist 192.168.1.1. Verwenden Sie den folgenden Befehl, um eine statische Route auf einem Computer der Filiale zu definieren:

```
route add 11.0.0.0 mask 255.0.0.0 192.168.1.1 -p
```

Einstellungen auf Remote-Clients überprüfen

Führen Sie die folgenden Schritte durch, um die Einstellungen auf einem entfernten Client zu überprüfen:

1. Melden Sie sich in Programm ViPNet Client als Administrator an.
2. Wählen Sie im Menü **Service** den Eintrag **Anwendungseinstellungen**.
3. Stellen Sie im Fenster **Einstellungen** sicher, dass das Kontrollkätschen **Firewall verwenden** im Bereich **Privates Netzwerk** aktiviert ist.
4. Klicken Sie auf **OK**.
5. Wählen Sie in der Navigationsleiste des Hauptfensters von ViPNet Client Monitor den Bereich **Privates Netzwerk**.
6. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf Coordinator A. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet.
7. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Firewall** (s. Abbildung 9 auf S. 23).
8. Stellen Sie sicher, dass die statische externe IP-Adresse der Firewall, hinter der sich Coordinator A befindet, in Tabelle **IP-Adressen** aufgelistet ist. Wenn die Firewall über keine statische IP-Adresse verfügt, überprüfen Sie den DNS-Namen der Firewall (Schritt **10**).
9. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **IP-Adresse** (s. Abbildung 8 auf S. 22).
10. Stellen Sie sicher, dass die lokale IP-Adresse des Coordinators A in der Tabelle **IP-Adresse** in Spalte **Reelle IP-Adressen** korrekt definiert ist.

    Falls DNS-Namen verwendet werden, stellen Sie sicher, dass das Kontrollkästchen **DNS-Name** verwenden aktiviert ist und der korrekte DNS-Name der Firewall, hinter der sich Coordinator A befindet, in der Liste **DNS-Name** angegeben ist.
11. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Tunnel** (s. Abbildung 16 auf S. 45).

    Stellen Sie sicher, dass das Kontrollkästchen **IP-Adressen zur Tunnelung verwenden** aktiviert ist und dass die IP-Adressen der getunnelten Knoten, die sich im Subnetz von Coordinator A befinden, aufgelistet sind.
12. Doppelklicken Sie im Bereich **Privates Netzwerk** in der Liste der Netzwerkknoten auf Coordinator B. Öffnen Sie im Fenster **Netzwerkknoten-Eigenschaften** die Registerkarte **Tunnel**. Stellen Sie sicher, dass das Kontrollkästchen **IP-Adressen zur Tunnelung verwenden** aktiviert ist und dass die IP-Adressen der getunnelten Knoten, die sich im Subnetz dieses Coordinators befinden, aufgelistet sind.

13 Überprüfen Sie die Verbindung zu jedem der Coordinatoren. Wählen Sie dazu den Coordinator im Bereich **Privates Netzwerk** aus und klicken entweder in der Symbolleiste auf die Schaltfläche **Verbindung** oder drücken die Taste **F5**.

14 Versuchen Sie nun, die Verbindung zu einem der getunnelten Knoten über seine IP-Adresse herzustellen (zum Beispiel mit Hilfe des Befehls `ping`).

Wenn alle Einstellungen richtig vorgenommen wurden, wird nun eine Verbindung zwischen dem entfernten Client und dem getunnelten Knoten hergestellt. Wenn keine Verbindung aufgebaut werden konnte, kann die Ursache in der Inkompatibilität der Softwareversionen oder in den Einstellungen der Firewall liegen. Wenden Sie sich an den technischen Support der Infotecs GmbH.

5

Verbindungen zwischen der Niederlassung und dem Benutzer eines mobilen Geräts

Kurze Übersicht 51

Netzwerkparameter in ViPNet Network Manager einstellen 53

Konfiguration des Coordinators unter Windows 56

Einstellungen auf externen Firewall überprüfen 58

Konfiguration mobiler Geräte 59

Einstellungen auf dem Coordinator unter Windows überprüfen 61

Kurze Übersicht

Dieses Kapitel beschreibt den Aufbau eines ViPNet VPN-Netzwerks, in dem Benutzer von Apple- und Android-Geräten Verbindungen zum Hauptniederlassung herstellen.

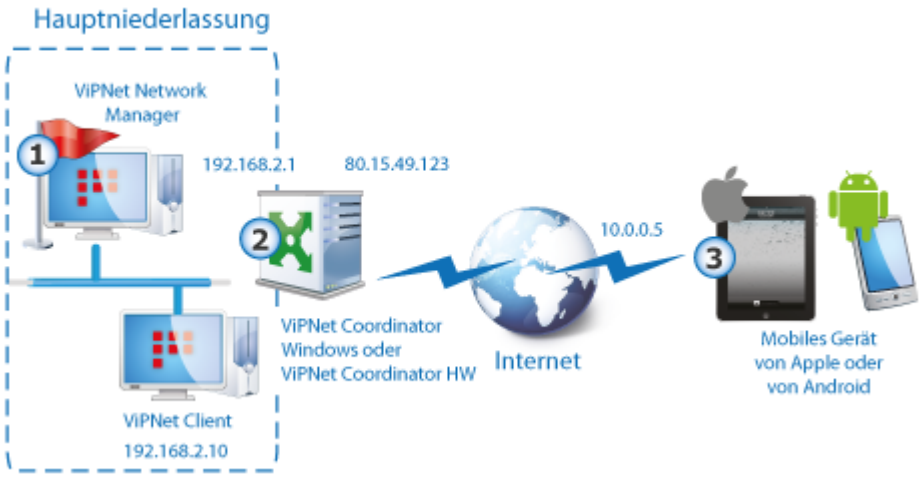

Abbildung 18. Verbindungen zwischen dem Zentrale und dem Benutzer eines mobilen Geräts

Die Verbindung zwischen dem offenen Netzwerkknoten und dem ViPNet Knoten erfolgt mit Hilfe des Coordinators, der die Rolle des Gateways ViPNet – IPsec übernimmt. Das -Gerät verbindet sich mit dem Coordinator über die Technologie IPsec. Dabei wird ein verschlüsselter Tunnel von diesem Gerät zum Coordinator aufgebaut. Dem -Gerät wird auf dem Coordinator eine IP-Adresse aus einem vorgegebenen Bereich (in der Abbildung 10.0.0.5) zugeordnet.

Auf dem Coordinator wird die Tunnelung des IP-Adressenbereichs, der die IPsec-Knoten umfasst, mit Hilfe der ViPNet Technologie verwirklicht. Auf diese Weise wird der IPsec-Knoten für die ViPNet Knoten entweder über die vom Coordinator vergebene IP-Adresse (in der Abbildung 10.0.0.5) oder die entsprechende virtuelle IP-Adresse des getunnelten Knotens erreichbar. Die ViPNet Knoten werden ihrerseits für den IPsec-Knoten über sichtbare Adressen auf dem Coordinator (in der Abbildung 192.168.2.10) erreichbar.

Bei Kommunikation von IPsec- und ViPNet Knoten nach diesem Schema sind zusätzliche Routing-Einstellungen auf den Knoten nicht erforderlich.

IP-Pakete, die vom -Gerät über die Technologie IPsec gesendet wurden, werden vom Coordinator entschlüsselt, anschließend vom ViPNet Treiber wieder verschlüsselt und über das geschützte ViPNet Netzwerk an den Ziel-Netzwerkknoten weitergeleitet. In gleicher Weise werden IP-Pakete in entgegengesetzter Richtung übertragen.

Der Coordinator, der die Rolle eines IPsec-Gateways übernimmt, muss folgende Anforderungen erfüllen:

- Coordinator einer der folgenden Typen:
  - ViPNet Coordinator HW/VA.
  - Windows-Coordinator mit dem Betriebsystem Windows Server 2008 R2.

Hinweis. Die Funktionen des IPsec-Gateways kann auch ein Computer mit dem Betriebssystem Windows Server 2003 übernehmen. Die in diesem Dokument enthaltenen Hinweise zur Konfiguration des IPsec-Gateways beziehen sich allerdings auf das Betriebssystem Windows Server 2008 R2.

Wenden Sie sich an den technischen Kundendienst von Infotecs GmbH, falls Sie Hilfe beim Konfigurieren des IPsec-Gateways unter Windows Server 2003 benötigen.

- Der Coordinator muss vom Internet aus über eine feste IP-Adresse oder einen DNS-Namen erreichbar sein (der Name kann mit Hilfe eines dynamischen DNS-Dienstes registriert werden).

Netzwerkparameter in ViPNet Network Manager einstellen

Erstellen Sie zuerst die erforderliche Struktur des ViPNet Netzwerks, wie im Abschnitt ViPNet Netzwerk einrichten (auf S. 16) beschrieben. Zum Implementieren des aufgeführten Schemas wird ein Netzwerk mit einem Coordinator, mehreren Clients und einem Smartphone-Client benötigt.

In diesem Abschnitt werden die wichtigsten Schritte bei der Konfiguration des IPsec-Gateways sowohl für einen Windows- als auch für einen ViPNet Coordinator HW/VA-Coordinator beschrieben. Wir empfehlen jedoch, einen ViPNet Coordinator HW/VA-Coordinator zu verwenden, da für die Konfiguration dieses Coordinators weniger Einstellungen notwendig sind. Die Konfiguration von ViPNet Coordinator HW/VA in ViPNet Network Manager ist nur dann möglich, wenn dies von der ViPNet Network Manager-Lizenz zugelassen ist.

Führen Sie in ViPNet Network Manager die folgenden Einstellungen durch (ausführliche Informationen zur Durchführung der aufgeführten Einstellungen finden Sie im Dokument „ViPNet VPN. Benutzerhandbuch" im Kapitel „Konfiguration von IPsec-Verbindungen mit mobilen Geräten und anderen Netzwerken"):

1. Wählen oder erstellen Sie einen ViPNet Coordinator Windows oder ViPNet Coordinator HW/VA, der die Rolle des IPsec-Gateways übernehmen soll.
2. Konfigurieren Sie in der Registerkarte **IPsec-Verbindung** die Parameter der Verbindung zum Coordinator unter Verwendung der IPsec-Technologie.

Abbildung 19. IPsec-Verbindungsparameter für Windows-Coordinator einstellen

3 Wenn der Zugang mobiler Geräte zu geschützten ViPNet Knoten ermöglicht werden soll, geben Sie einen Bereich von getunnelten Adressen für die Smartphone-Clients an.

4 Fügen Sie einen Smartphone-Client auf dem Coordinator hinzu und konfigurieren Sie ein IPsec-Profil für diesen Smartphone-Client auf der Registerkarte **Profil**.

Obwohl in der Dropdownliste **Typ des Smartphone-Clients** nur der Eintrag **iOS** zur Verfügung steht, sollten die Werte der anderen Parameter auch dann definiert werden, wenn die Verbindung über ein Android-Gerät erfolgen soll. Dies wird damit begründet, dass die aufgeführten Parameter auf dem Coordinator, der als IPsec-Gateway auftritt, verwendet werden.

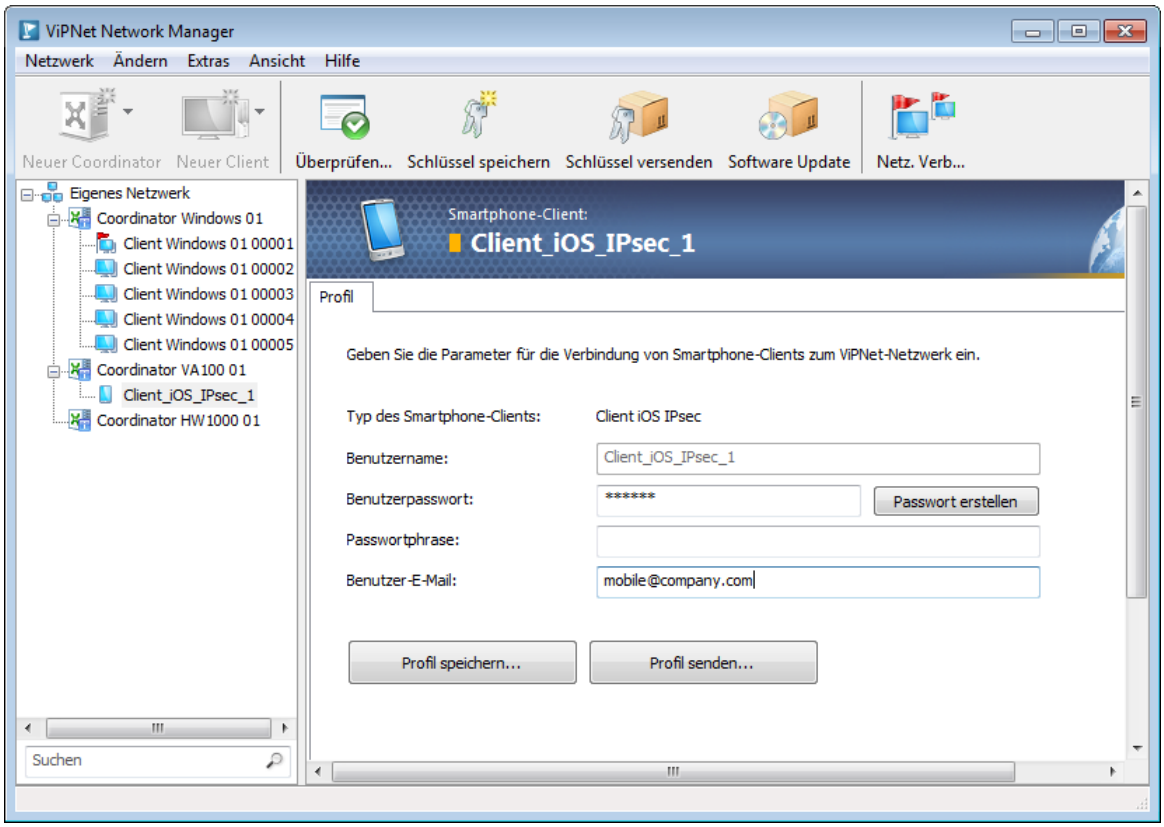

Abbildung 20. Parameter des Smartphone-Clients

5 Wenn ein Apple-Gerät als Smartphone-Client auftritt, senden Sie das konfigurierte Profil an das mobile Gerät.

6 Wenn ein Windows-Coordinator als IPsec-Gateway festgelegt ist, speichern Sie das Profil, das in der Registerkarte **IPsec-Verbindung** des Coordinators konfiguriert wurde.

7 Wenn ein ViPNet Coordinator HW/VA-Coordinator als IPsec-Gateway festgelegt ist, senden Sie die Schlüssel an den ViPNet Coordinator HW/VA-Coordinator.

   Wenn auf dem Coordinator keine Schlüssel installiert sind, erstellen Sie eine Schlüsseldistribution für den Coordinator und leiten diese zusammen mit der Datei `hwinit_set.xml` an den Administrator des Coordinators weiter.

Falls ein ViPNet Coordinator HW/VA-Coordinator verwendet wird, gehen Sie anschließend zur Konfiguration des mobilen Geräts über (s. Konfiguration mobiler Geräte auf S. 59). Falls ein Windows-Coordinator verwendet wird, konfigurieren Sie zunächst den Coordinator (s. Konfiguration des Coordinators unter Windows auf S. 56) und gehen Sie anschließend zur Konfiguration des mobilen Geräts über.

Konfiguration des Coordinators unter Windows

Führen Sie auf einem Coordinator mit dem Betriebssystem Windows Server 2008 R2 die folgenden Schritte aus:

1 Starten Sie im Snap-In **Server-Manager** den Assistenten zum Hinzufügen von Rollen und installieren die Rolle **Netzwerkrichtlinien- und Zugriffsdienste**, indem Sie für diese Rolle die Komponente **Routing- und RAS-Dienste** auswählen.

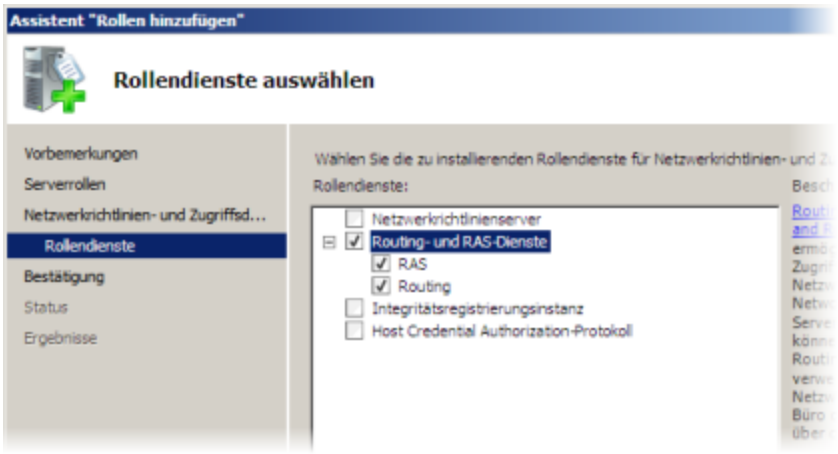

Abbildung 21. Dienste für die Installation auswählen

2 Starten Sie im Snap-In **Server-Manager** den Dienst „Routing und RAS“, indem Sie im Setup-Assistenten die Konfiguration **RAS (DFÜ oder VPN)** auswählen.

Setup-Assistent für den Routing- und RAS-Server
Konfiguration
Sie können eine beliebige Kombination an Diensten wählen, oder Sie können diesen Server benutzerdefiniert anpassen.
RAS (DFÜ oder VPN)
Ermöglicht Remoteclients, eine Verbindung mit diesem Server über eine DFÜ-Verbindung oder eine sichere VPN-Internetverbindung herzustellen.
Netzwerkadressübersetzung (NAT)
Ermöglicht internen Clients, eine Internetverbindung mit einer einzelnen öffentlichen IP-Adresse herzustellen.
VPN-Zugriff und NAT
Ermöglicht Remoteclients, eine Verbindung mit diesem Server über das Internet, und lokalen Clients eine Internetverbindung über eine einzige öffentliche IP-Adresse herzustellen.
Sichere Verbindung zwischen zwei privaten Netzwerken
Verbindet dieses Netzwerk mit einem Remotenetzwerk, wie z.B. einer Zweigstelle.
Benutzerdefinierte Konfiguration
Wählen Sie eine beliebige Routing- und RAS-Featurekombination aus.
Weitere Informationen
< Zurück
Weiter >
Abbrechen

Abbildung 22. Konfiguration auswählen

3 Übernehmen Sie auf dem Coordinator das für diesen Coordinator in ViPNet Network Manager erstellte IPsec-Profil, indem Sie die Datei `run.bat` starten.

4 Konfigurieren Sie im Programm ViPNet Coordinator einen lokalen Filter des offenen Netzwerks, der die Anbindung mobiler Geräte unter Verwendung der IPsec-Technologie erlaubt. Dabei:

   - legen Sie **Mein ViPNet Knoten** und den Netzwerkadapter des Coordinators, der mit dem Internet verbunden ist, als Ziel fest;
   - fügen Sie das IP-Protokoll `50 - ESP` sowie die UDP-Protokolle `500-isakmp` und `4500` hinzu.

5 Wenn der Zugriff mobiler Clients auf die Ressourcen unmittelbar auf dem Coordinators ermöglicht werden soll, dann konfigurieren Sie lokaler Filter des offenen Netzwerks für die Weiterleitung des Traffics über entsprechende Protokolle und Ports. Dabei:

   - geben Sie als Quelle den IP-Adressbereich an, aus dem Adressen an mobile Geräte bei ihrer Verbindung zum Coordinator zugewiesen werden und der in ViPNet Network Manager bei der Konfiguration des IPsec-Gateways festgelegt wurde;
   - legen Sie **Mein ViPNet Knoten** als Ziel fest;
   - fügen Sie das TCP-Protokoll `80-http` hinzu.

6 Nachdem Sie alle Filter konfiguriert haben, klicken Sie im Bereich **Lokale Filter des offenen Netzwerks** auf **Alle übernehmen**.

7 Wenn der Zugriff mobiler Geräte auf ViPNet Netzwerkknoten über DNS-Namen erfolgen soll, installieren und konfigurieren Sie auf dem Coordinator einen DNS-Server und registrieren dort die DNS-Namen von ViPNet Netzwerkknoten (siehe das Dokument „ViPNet VPN. Benutzerhandbuch", Kapitel „Einstellung und Verwendung der DNS- und WINS-Dienste im ViPNet Netzwerk").

Einstellungen auf externen Firewall überprüfen

Wenn der Coordinator über eine externe Firewall mit dem Internet verbunden ist, sollte auf dieser Firewall (oder DSL-Router) eine Regel für UDP-Pakete konfiguriert werden, die im Zuge der Kommunikation über das IPsec- oder L2TP-Protokoll ausgetauscht werden.

Führen Sie dazu eine der folgenden Aktionen aus:

- Stellen Sie sicher, dass auf dem Gerät, das als externe Firewall benutzt wird, die Optionen L2TP Passthrough und IPsec Passthrough aktiviert sind (falls diese Parameter vom entsprechenden Gerät unterstützt werden).

  Danach sind keine weiteren Aktionen mehr erforderlich.

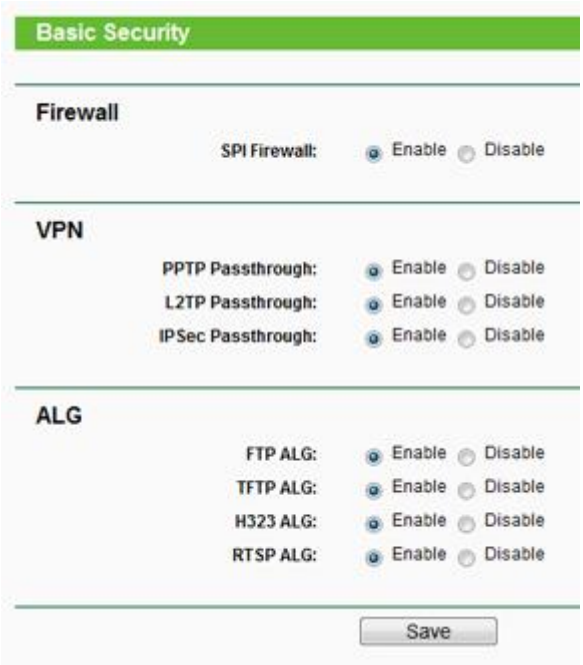

Abbildung 23. Routing-Parameter

- Falls die Parameter L2TP Passthrough und IPsec Passthrough von Ihrem Gerät nicht unterstützt werden, konfigurieren Sie die Regel manuell, indem Sie folgende Parameterwerte verwenden:
  - IP-Adresse des Servers auf dem die Software ViPNet Coordinator installiert ist und zu dem die Portweiterleitung erfolgen soll.
  - Protokoll: UDP.
  - Ports: 500 und 4500.

Konfiguration mobiler Geräte

Konfiguration mobiles Geräts von Apple

Profile für Smartphone-Client, der im ViPNet Network Manager erstellt wurde, muss auf dem Apple-Gerät installiert werden.

1. Öffnen Sie auf dem Gerät iPad oder iPhone die Nachricht, die das versendete IPsec-Profil als Anhang enthält (Datei mit Erweiterung `.mobileconfig`).
2. Wählen Sie die angehängte Datei aus. Es wird das Fenster zur Installation des Profils geöffnet.
3. Klicken Sie auf **Installieren**. Beim Einblenden einer Warnung, dass das Profil nicht signiert ist, klicken Sie erneut auf **Installieren**.
4. Geben Sie im Passwort-Fenster das Benutzerkennwort ein, das für diesen Smartphone-Client in ViPNet Network Manager angelegt wurde. Dieses Passwort können Sie beim Administrator des ViPNet Netzwerks anfordern.
5. Nach Eingabe des Passworts ist die Installation des Profils abgeschlossen. Klicken Sie auf **Fertig**.
6. Öffnen Sie das Programm **Einstellungen** und wählen Sie in der Navigationsleiste den Bereich **VPN**, um die Parameter des installierten Profils zu konfigurieren.
7. Wählen Sie in der Panel-Ansicht das installierte IPsec-Profil.
8. Klicken Sie im Fenster mit den Profileigenschaften im Bereich **Proxy** auf **Aus**.
9. Klicken Sie auf **Sichern**.

   Die Installation und die Konfiguration des Profils sind nun abgeschlossen.

Zum Aufbau einer Verbindung zum ViPNet Netzwerk öffnen Sie das Programm **Einstellungen** und wählen **Allgemeine** > **Netzwerk** > **VPN**, dann setzen Sie den Schalter auf .

Wenn Sie auf Objekte im geschützten Netzwerk zugreifen möchten, geben Sie in der Adresszeile des Browsers oder einer anderen Anwendung die IP-Adresse oder den DNS-Namen des geschützten ViPNet Knotens ein.

Konfiguration mobiles Geräts von Android

Um ein Android-Gerät zu geschützten Unternehmensressourcen zu verbinden, führen Sie folgende Aktionen durch:

1. Fügen Sie ein IPsec-Profil auf Ihrem Android-Gerät hinzu:

   1.1 Klicken Sie auf das Menü **Einstellungen** > **Wireless & Networking** > **VPN**.

   1.2 Erstellen Sie ein neues VPN-Profil.

   1.3 Legen Sie als Verbindungstyp **L2TP/IPSec PSK** fest.

1.4 Geben Sie zum Festlegen der Serveradresse die IP-Adresse oder den DNS-Namen des ViPNet Coordinator HW/VA-Knotens, die Sie in ViPNet Network Manager definiert haben, auf der Registerkarte **IPsec-Verbindung** ein.

1.5 Geben Sie zum Festlegen des Pre-Shared Keys den Pre-Shared Key, den Sie auf der Registerkarte **IPsec-Verbindung** (s. Abbildung 19 auf S. 54) angegeben haben, ein.

1.6 Speichern Sie das VPN-Profil.

2 Tippen Sie auf das erstellte VPN-Profil. Die Benutzer-Anmeldeinformationen werden angefordert:

2.1 Geben Sie den Benutzernamen, den Sie in ViPNet Network Manager definiert haben, auf der Eigenschaften-Registerkarte des Smartphone-Clients ein.

2.2 Geben Sie das Passwort, das Sie in ViPNet Network Manager definiert haben, auf der Eigenschaften-Registerkarte des Smartphone-Clients ein.

2.3 Tippen Sie auf **Verbinden**.

Hinweis. Die Bezeichnung und Anordnung der aufgelisteten Optionen kann sich auf Ihrem Android-Gerät von der hier genannten unterscheiden.

Einstellungen auf dem Coordinator unter Windows überprüfen

Führen Sie die folgenden Schritte aus, um die Einstellungen auf dem Windows-Coordinator zu überprüfen:

Überprüfen Sie die Adressen für die Tunnelung.

1 Wählen Sie im Hauptfenster des Programms ViPNet Coordinator den Menübefehl **Service** > **Anwendungseinstellungen**.

2 Wählen Sie im Fenster **Einstellungen** den Bereich **Tunnelung** und stellen sicher, dass in diesem Bereich jene Adressen aufgelistet sind, die in ViPNet Network Manager für den Coordinator in der Registerkarte **Tunnel** angegeben wurden.

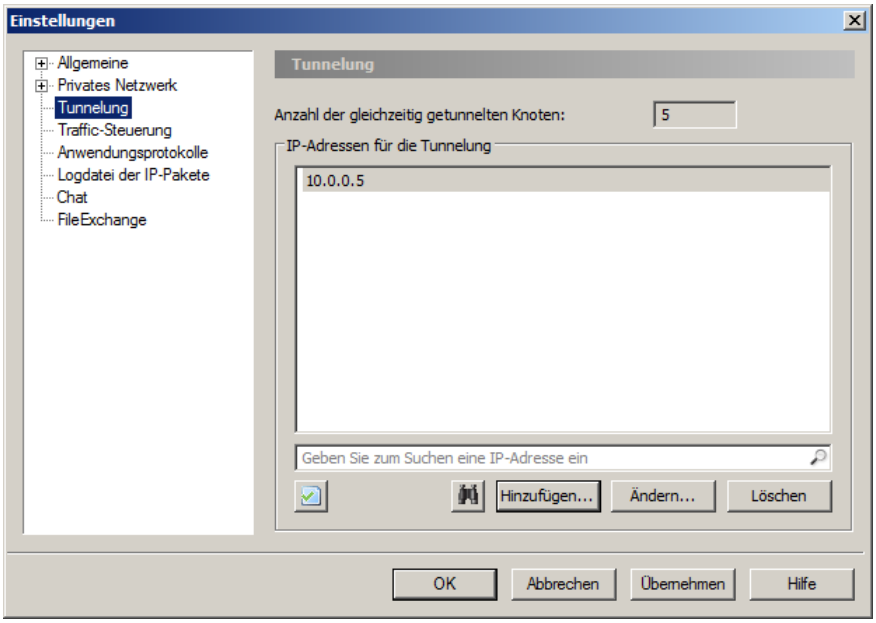

Abbildung 24. Überprüfen der Einstellungen für die Tunnelung auf dem Coordinator

3 Überprüfen Sie die Liste der lokalen Benutzer.

- Wählen Sie auf dem Computer mit installierter ViPNet Coordinator-Software im Menü **Start** den Eintrag **Verwaltung** > **Computerverwaltung**.
- Klicken Sie im Snap-In **Computerverwaltung** in der linken Leiste auf den Eintrag **Verwaltungstools** > **Lokale Benutzer und Gruppen** > **Benutzer**.
- Stellen Sie sicher, dass in der Benutzerliste der Benutzer enthalten ist, dessen Namen Sie in ViPNet Network Manager in der Registerkarte mit den Einstellungen des Smartphone-Clients angegeben haben (s. Abbildung 20 auf S. 55).

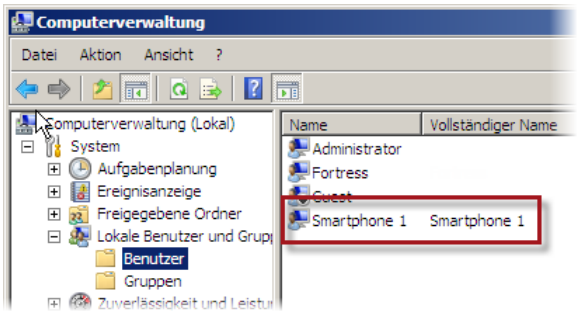

Abbildung 25. Überprüfen des Benutzerkontos für den Smartphone-Client

4 Überprüfen Sie die Einstellungen des Dienstes „Routing und RAS".

- Wählen Sie auf dem Computer mit installierter ViPNet Coordinator-Software im Menü **Start** den Eintrag **Verwaltung** > **Server-Manager**.
- Klicken Sie im Snap-In **Server-Manager** in der linken Leiste mit der rechten Maustaste auf den Eintrag **Rollen** > **Netzwerkrichtlinien- und Zugriffsdienste** > **Routing und RAS** und wählen im Kontextmenü **Eigenschaften**.
- Stellen Sie sicher, dass in den Einstellungen des Dienstes der gleiche Wert für den voreingestellten Schlüssel (Pre-Shared Key) eingetragen ist, den Sie in ViPNet Network Manager angegeben haben

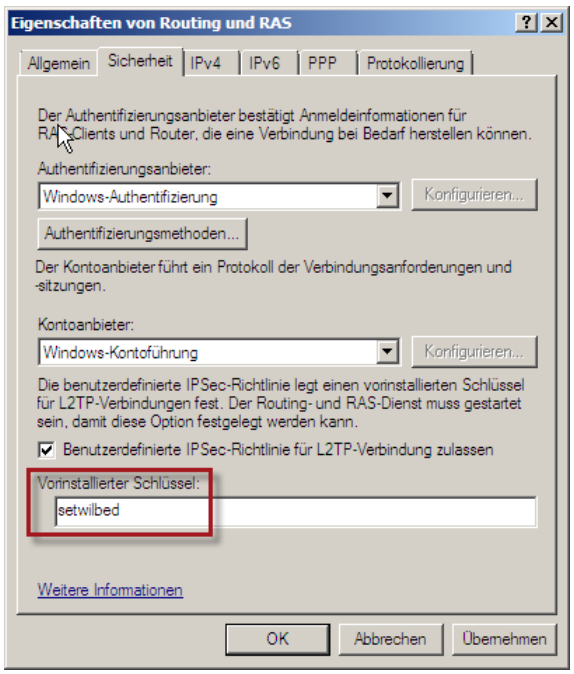
Eigenschaften von Routing und RAS
Allgemein Sicherheit IPv4 IPv6 PPP Protokollierung
Der Authentifizierungsanbieter bestätigt Anmeldeinformationen für RAS-Clients und Router, die eine Verbindung bei Bedarf herstellen können.
Authentifizierungsanbieter:
Windows-Authentifizierung
Konfigurieren...
Authentifizierungsmethoden...
Der Kontoanbieter führt ein Protokoll der Verbindungsanforderungen und -sitzungen.
Kontoanbieter:
Windows-Kontoführung
Konfigurieren...
Die benutzerdefinierte IPSec-Richtlinie legt einen vorinstallierten Schlüssel für L2TP-Verbindungen fest. Der Routing- und RAS-Dienst muss gestartet sein, damit diese Option festgelegt werden kann.
Benutzerdefinierte IPSec-Richtlinie für L2TP-Verbindung zulassen
Vorinstallierter Schlüssel:
setwilbed
Weitere Informationen
OK
Abbrechen
Übernehmen

Abbildung 26. Überprüfen der Einstellungen des Dienstes „Routing und RAS"

6

Verbindungen zwischen zwei Niederlassungen unter Verwendung von ViPNet und IPsec-Technologie

Kurze Übersicht 64

Netzwerkparameter in ViPNet Network Manager einstellen 65

Überprüfen der Einstellungen auf dem Remotegateway 69

Kurze Übersicht

Dieses Kapitel beschreibt die Reihenfolge der Konfiguration von Verbindungen zwischen dem ViPNet VPN-Netzwerk und einem anderen Netzwerk, in dem keine ViPNet Technologie verwendet wird.

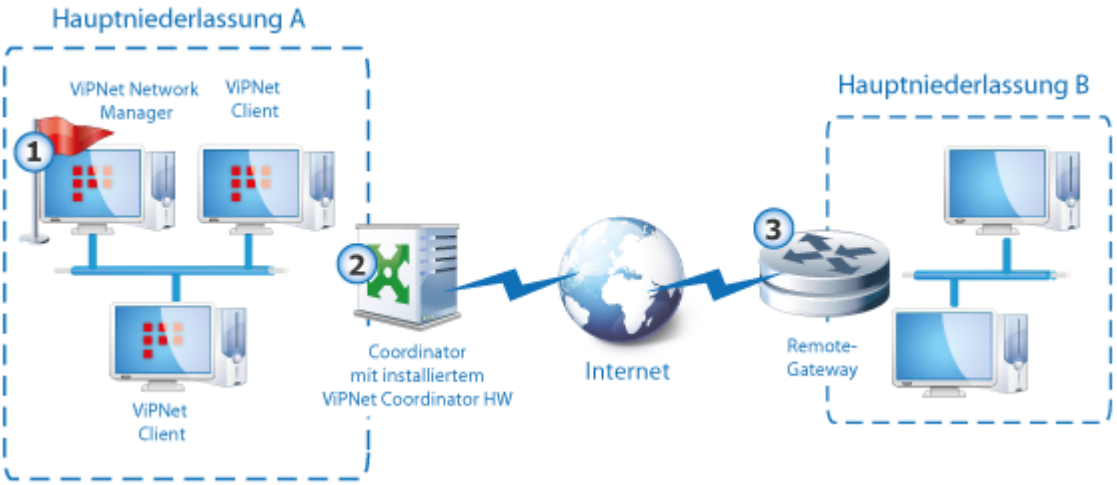

Abbildung 27. Verbindung zwischen zwei Büros unter Verwendung von ViPNet- und IPsec-Technologie

Nehmen wir an, dass Ihr Firmennetzwerk durch ein ViPNet VPN geschützt ist. Sie möchten einen abgesicherten Kanal für die Kommunikation mit einer Partnerfirma einrichten, die keine ViPNet Technologie verwendet.

In diesem Fall kann ein Tunnel zwischen den zwei unternehmensinternen Netzwerken unter Verwendung des IPsec-Protokolls eingerichtet werden. Ein IPsec-Tunnel ist ein verschlüsselter Traffic-Tunnel zwischen zwei IPsec-Gateways (ein IPsec-Gateway befindet sich in jedem der zwei Netzwerke). Es steht eine Vielzahl an IPsec-Gateway Softwareservern und Geräten zur Verfügung (Cisco-Geräte, Server mit Linux, FreeBSD, Windows-Server, u. s. w.).

Ein ViPNet Coordinator HW/VA-Knoten kann ebenfalls als das IPsec-Gateway Ihres Netzwerks verwendet werden.

Hinweis. Die Konfiguration eines Windows-Coordinators als ViPNet IPsec-Gateway für den Aufbau von Partnernetzwerk-Verbindungen mit einem anderen Netzwerk wird vom Programm ViPNet Network Manager nicht unterstützt.

Ein Netzwerkknoten ViPNet Coordinator HW/VA, der als IPsec-Gateway auftritt, wird unmittelbar im Programm ViPNet Network Manager konfiguriert. Eine solche Konfiguration kann nur dann durchgeführt werden, wenn die Verwendung von ViPNet Coordinator HW/VA von der ViPNet Network Manager-Lizenz zugelassen ist.

Netzwerkparameter in ViPNet Network Manager einstellen

Führen Sie zuerst die folgenden Schritte aus:

1. Erstellen Sie die erforderliche Struktur des ViPNet Netzwerks, wie im Abschnitt ViPNet Netzwerk einrichten (auf S. 16) beschrieben ist.
2. Stellen Sie sicher, dass die Verwendung von ViPNet Coordinator HW/VA von der ViPNet Network Manager-Lizenz zugelassen ist. Wenden Sie sich anderenfalls an einen Vertreter von „Infotecs“ und bestellen Sie eine neue ViPNet Netzwerklizenz.
3. Erstellen Sie die Schlüssel für den ViPNet Coordinator HW/VA und installierten die Schlüssel auf diesen Coordinator.

Wählen Sie in ViPNet Network Manager in der Navigationsleiste den ViPNet Coordinator HW/VA aus und führen die folgenden Einstellungen durch:

1. Wechseln Sie in der Panel-Ansicht zur Registerkarte **IPsec-Verbindung**.
2. Wählen Sie in der Liste **Netzwerkadaptername** denjenigen Netzwerkadapter auf dem ViPNet Coordinator HW/VA-Knoten aus, der aus dem Internet erreichbar ist.
3. Aktivieren Sie das Kontrollkästchen **Coordinator für geschützte IPsec-Verbindung anderer Netzwerke verwenden**.

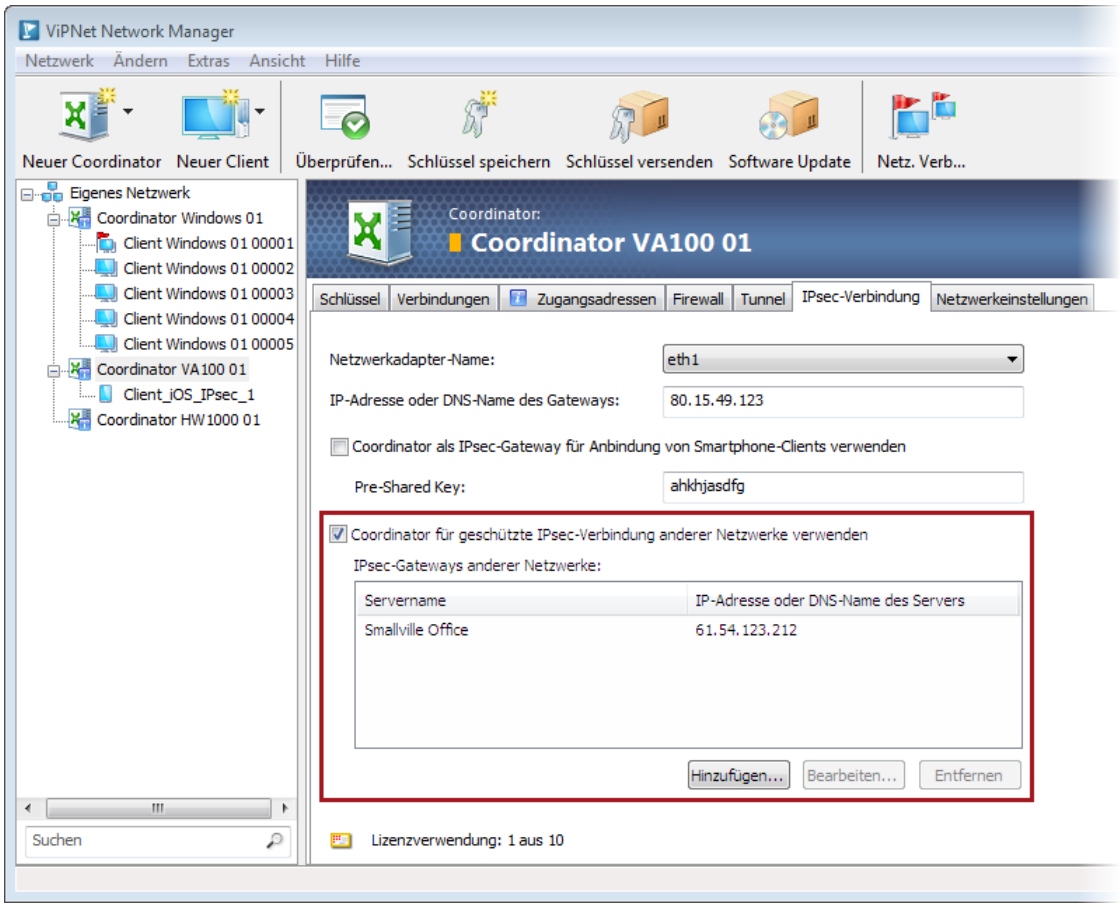

Abbildung 28. Hinzufügen eines IPsec-Kanals zu einem anderen Netzwerk

4 Klicken Sie auf **Hinzufügen**, um einen neuen IPsec-Kanal zum Remotenetzwerk zu konfigurieren. Das Fenster **IPsec-Gateway Neu** wird geöffnet.

5 Geben Sie auf der Registerkarte **Verbindung** im Feld **Remotegateway-Name** einen eindeutigen Namen für die Verbindung zum Remotenetzwerk an.

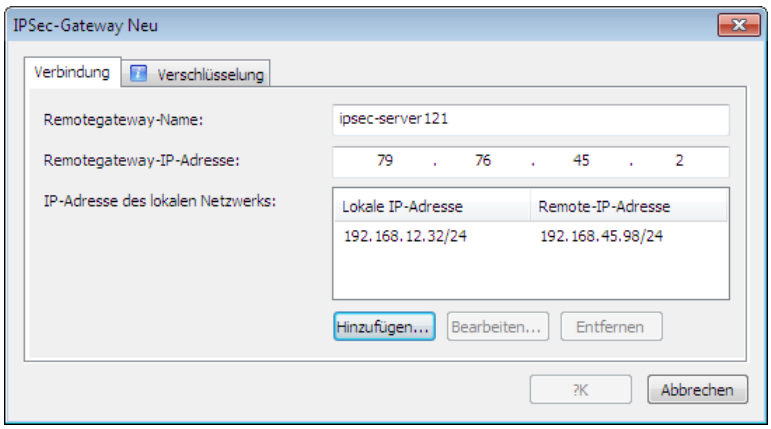

Abbildung 29. Angeben der Parameter für remote IPsec-Gateway

6 Geben Sie im Feld **Remotegateway-IP-Adresse** die Zugangsadresse des entfernten IPsec-Gateways an.

7 Klicken Sie auf **Hinzufügen**. Definieren Sie im Fenster **Adressen des lokalen und Remotenetzwerks** die IP-Adressen der Netzwerke, die mittels IPsec-Kanal miteinander verbunden werden sollen. Netzwerkadressen sollten in der CIDR-Notation angegeben werden, zum Beispiel 172.16.0.0/24.

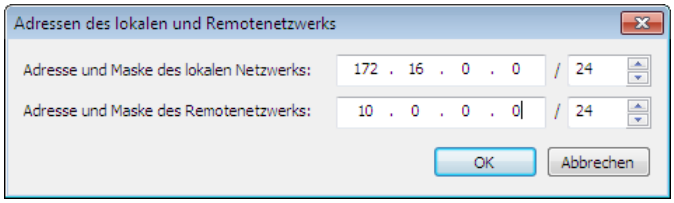
Adressen des lokalen und Remotenetzwerks
Adresse und Maske des lokalen Netzwerks:
172 . 16 . 0 . 0 / 24
Adresse und Maske des Remotenetzwerks:
10 . 0 . 0 . 0 / 24
OK
Abbrechen

Abbildung 30. Festlegen des lokalen und Remotenetzwerks

Wenn nötig, wiederholen Sie diesen Schritt, um weitere Paare von lokalen und Remotenetzwerken zu erstellen.

8 Öffnen Sie die Registerkarte Verschlüsselung und konfigurieren Sie die Verschlüsselungsparameter der Verbindung:

- Geben Sie im Feld **Pre-Shared Key** eine beliebige Reihenfolge an Zeichen ein (8 bis 63 Zeichen lang). Diese Zeichenfolge wird als Passwort für die Verbindungsauthentifizierung verwendet.

Achtung! Der Pre-Shared Key darf die folgenden Zeichen nicht enthalten: Fragezeichen (?), umgekehrter Schrägstrich (\), einfaches Anführungszeichen (').

- Wenn nötig, geben Sie den Verschlüsselungs- und Hashalgorithmus, den Diffie-Hellman-Parameter und die Gültigkeitsdauer der Schlüssel in den entsprechenden Feldern an.

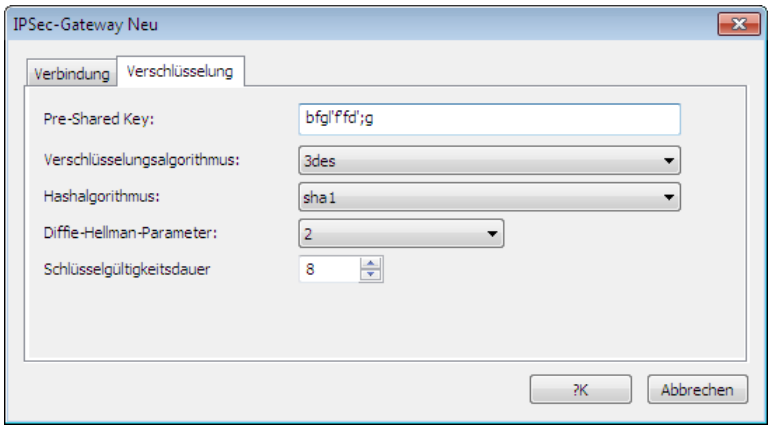

Abbildung 31. Definition der Verschlüsselungsparameter

Achtung! Informieren Sie den Administrator des Remotenetzwerks, dass die gleichen Verschlüsselungsparameter auf dem Remotegateway eingestellt werden sollen.

9 Klicken Sie in der Panel-Ansicht auf der Registerkarte **Schlüssel** auf **Schlüssel senden**, um die IPsec-Verbindungseinstellungen an den ViPNet Coordinator HW/VA-Knoten zu übertragen.

10 Senden Sie dann die Schlüssel auf den ViPNet Coordinator HW/VA-Knoten und konfigurieren eine Transitregel, die den Traffic-Austausch zwischen dem ViPNet Netzwerk und dem Remotenetzwerk erlaubt.

Überprüfen der Einstellungen auf dem Remotegateway

Kontaktieren Sie den Administrator des Remotenetzwerks und stellen Sie sicher, dass auf dem Gateway des Remotenetzwerks die gleichen Verschlüsselungsparameter (Pre-Shared Key, Verschlüsselungs- und Hashalgorithmus und andere Parameter) eingestellt sind, wie in den IPsec-Verbindungseinstellungen von ViPNet Network Manager.